



DEPARTMENT CRITICAL INFRASTRUCTURE PROTECTION IMPLEMENTING PLANS TO PROTECT CYBER-BASED INFRASTRUCTURE

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 04-05
November 2003

DEPARTMENT CRITICAL INFRASTRUCTURE PROTECTION IMPLEMENTING PLANS TO PROTECT CYBER-BASED INFRASTRUCTURE

EXECUTIVE SUMMARY

The Department of Justice (Department) and other government departments and agencies are required to prepare and implement plans for protecting critical infrastructure. The infrastructure includes systems essential to the minimum operations of the economy and government, such as telecommunications, banking and finance, energy, and transportation. According to the Critical Infrastructure Assurance Office's (CIAO) National Plan for Information Systems Protection, the threat is that a group or nation hostile to the United States will seek to "inflict economic damage, disruption and death, and degradation of our defense response" by attacking our critical infrastructure.¹ Critical infrastructure protection plans are required to include an inventory of the Department's mission-essential assets, an assessment of each asset's vulnerabilities, and plans to remediate those vulnerabilities.

In May 1998, Presidential Decision Directive 63 (PDD 63) required all federal agencies to achieve and maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish their ability to perform essential national security missions and ensure general public health and safety. Achieving and maintaining this ability is referred to as "full operating capability." PDD 63 required the Department to reach full operating capability by May 2003.

The National Plan for Information Systems Protection, Version 1.0, issued by the CIAO in 2000, describes full operating capability as the ability to ensure that any interruption or manipulation of critical functions is ". . . brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States." Further, the Draft Critical Infrastructure Protection (CIP) Plan indicates that full operating capability for the Department is comprised of:

¹ The CIAO was created in May 1998 to coordinate the federal government's initiatives on infrastructure assurance.

- identifying the Minimum Essential Infrastructure (MEI) and interdependencies and identifying and addressing their vulnerabilities,²
- detecting attacks and unauthorized intrusions,
- sharing attack warning and information in a secure and timely manner, and
- responding to attacks and reconstituting and recovering assets that were subject to attacks.

The Department of Justice Office of the Inspector General (OIG) previously audited the adequacy of the Department's planning and assessment activities for protecting its critical computer-based infrastructure. Over 20 Inspectors General conducted similar audits of their own agencies as part of an effort sponsored by the President's Council on Integrity and Efficiency (PCIE). Our November 2000 report noted that the Department had submitted its initial critical infrastructure protection plan to the CIAO as required, and the Department had revised its initial plan according to comments received from an Expert Review Team. However, we concluded that the Department had not yet: 1) adequately identified all of its mission-essential assets, 2) assessed the vulnerabilities of each of its assets, 3) developed remedial action plans for identified vulnerabilities, and 4) developed a multi-year funding plan for reducing vulnerabilities. As a result, the Department's ability to perform certain vital missions was at risk from terrorist attacks or similar threats.

Our current audit of critical infrastructure protection is a continuation of the executive branch-wide effort by the PCIE. We, along with other OIGs, who are conducting similar audits, focused on the adequacy of implementation activities for protecting critical computer-based infrastructures. Specifically, we reviewed Department activities in the areas of: risk mitigation; emergency management; interagency coordination; resource and organization requirements; the recruitment, education of Information Technology (IT) personnel; and computer security awareness. In addition, we reviewed follow-up activities undertaken with regard to the recommendations of our November 2000 report and found that the

² The MEI is the framework of critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes essential to accomplishing an organization's core mission as those missions relate to national security, national economic security, or continuity of government services.

Department has made progress in the implementation of its CIP Plans, but much significant work remains to be done.

Background

Within the Department, the Justice Management Division (JMD) develops, promulgates, and reviews implementation of departmentwide policies, standards, and procedures for the management of automated information processing resources. Within JMD, the Chief Information Officer (CIO) has oversight responsibility for CIP for the Department. Within the Office of the CIO, the Information Technology Security Staff (ITSS) has primary responsibility for critical infrastructure planning and implementation.³

In May 2003, the CIO reorganized the information resource management function. At that time, the ITSS was established, and it is now responsible for developing and implementing policies and procedures for information systems security programs. Prior to the reorganization, these functions were managed by the Information Management and Security Staff (IMSS). Upon its establishment, the ITSS retained the prior staff and oversight responsibilities of the IMSS. The ITSS also gained responsibility from JMD Computer Services Staff (CSS) for managing the Department of Justice Computer Emergency Response Team (DOJCERT). The DOJCERT assists component organizations with incident handling and resolution, and it is the centralized reporting entity for the Department. All components are required to report computer security incidents to the DOJCERT and the DOJCERT issues any necessary alerts to components and external agencies.

Within the Department, critical infrastructure protection is a shared responsibility between JMD and the various component organizations. Each component is responsible for identifying its MEI, assessing vulnerabilities, developing remediation and funding plans, and ensuring the implementation of the plans. JMD is responsible for coordinating the departmentwide effort and ensuring that the components comply with applicable requirements.

³ Prior to September 11, 2002, JMD Security and Emergency Planning Staff had oversight of IT security for the classified systems of the Department, while the CIO's Information Management and Security Staff had oversight for the sensitive but unclassified systems. After September 11, 2002, the CIO is responsible for overseeing and implementing security policy and practices for both classified and sensitive but unclassified systems. The standards, procedures, and guidelines are coordinated with the Department's Security Officer.

Risk Mitigation

The Department is required to conduct vulnerability assessments to identify risks to its critical infrastructure. After the vulnerability assessments, remedial action plans are required to mitigate the exploitation of risks until the vulnerabilities are eliminated or reduced to an acceptable level. The remedial action plans should be system specific and should identify the vulnerability, responsible office, mission impact, mitigation action, long-term correction, and estimated costs and milestones for corrective measures.

JMD completed a vulnerability assessment in March 2002. JMD reviewed the management controls developed to implement the Department's CIP program and evaluated the controls against requirements contained in reports and other documents from the General Accounting Office, the National Critical Infrastructure Assurance Office, and the General Services Administration. The JMD review identified the following four individual vulnerabilities associated with the program.

1. The CIP Plan needed to be updated to incorporate the implementation plan and the Department's new Strategic Plan.
2. The inventory of mission-essential assets required revalidation by components after the events of September 11, 2001.
3. JMD needed to address the risk of not meeting the full operating capability date of May 2003.
4. Seven of the mission-essential systems required an independent certification and accreditation.

As previously mentioned, the National Plan for Information Systems Protection, Version 1.0, issued by the CIAO describes full operating capability as the ability to ensure that any interruption or manipulation of critical functions is "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States." Several items remain to be completed before the Department can reach full operating capability. In July 2002, IMSS officials indicated that mitigation action for all program vulnerabilities was progressing on target and would be completed on schedule. However, we found that the IMSS did not effectively manage the mitigation actions because it did not provide components sufficient time to provide required data to revalidate the MEI.

Another item we found that prevented the Department from reaching full operating capability was that project plans were not developed to ensure full operating capability by May 2003. In April 2003, we updated our assessment of progress by the IMSS/ITSS and found that project plans had been completed and included in the revised draft CIP Plan. However, those plans did not include completion dates for all tasks, and 54 of 73 tasks were not completed by May 2003. However, in our judgment four key tasks prevent the Department from achieving full operating capability. The four tasks are:

- development of contingency plans for systems without plans or revision of inadequate plans,
- testing of the contingency plans,
- incorporation of vulnerabilities into the Security and Management Reporting Tool (SMART) database for tracking purposes,⁴ and
- development of a SMART database for classified systems.

As a result of these tasks not being completed timely, the Department has less than adequate assurance that critical IT asset vulnerabilities will be mitigated adequately or timely.

Emergency Management

The Department's April 1999 CIP Plan established the critical elements for an effective emergency management program and charged a CIP Task Force with its implementation.⁵ The Department's emergency management program, as envisioned in the CIP Plan, was to incorporate the elements of Indications and Warnings; Incident Collection, Reporting, and Analysis; and Response and Contingency Plans.

⁴ The SMART database is a set of user interface, database management, and business intelligence tools designed to assist the Department CIO and program managers as well as the security administrators in identifying, controlling, and monitoring the performance of a component's IT security program and its IT systems.

⁵ The CIP Task Force was comprised of representatives from law enforcement, litigating divisions, and administrative offices.

Regarding Indications and Warnings, the plan intended to establish an effective and secure mechanism for: a) receiving threat indication and warning information from the intelligence community and law enforcement agencies concerning the critical infrastructure of the Department and the nation, and b) disseminating this information in a timely manner to appropriate Department components. The IMSS was to ensure the existence of secure, effective, and timely communication channels for passing threat information from internal and external organizations to Department components at both headquarters and field locations charged with the protection of the Department's critical infrastructure assets.

Regarding Incident Collection, Reporting, and Analysis, the Plan intended to define and establish an effective and secure mechanism for collecting, reporting, and analyzing incident information about actual and potential attacks on the Department's critical infrastructure assets. The established method should have ensured that information generated from computer security incidents was received from Department components and disseminated throughout the Department and to other intelligence and law enforcement agencies, as appropriate, in a timely manner.

Regarding Response and Contingency Plans, the Plan intended to define and establish sound response and contingency plans to ensure the Department's critical infrastructure assets could be restored to the minimum operational effectiveness necessary to support the Department's missions should these critical infrastructure assets be subjected to successful attack. Response plans identify actions for responding to a significant infrastructure attack while the attack is underway. Contingency plans identify actions required to rebuild or restore an infrastructure after it has been damaged. The CIP Plan required that response and contingency plans should be prepared, reviewed, and approved by Department officials, and be exercised on a periodic basis to ensure that the plans can be effectively implemented.

The CIP Plan also established several intermediate milestones for implementing the three essential elements of the Department's emergency management program. Full implementation of the program was to occur no later than September 28, 1999.

Although the April 1999 CIP Plan contained a comprehensive blueprint and milestones for an effective, centrally managed Department emergency management program, we found that such a program was not fully implemented. Many of the critical emergency management program elements relating to indications and warnings, incident collection, reporting

and analysis, and response and contingency planning were neither established nor operating.

Communication channels were established for passing threat information, but the IMSS did not determine whether the channels were secure, effective, and provided timely information as required by the CIP Plan. Additionally, the IMSS did not verify whether effective liaisons with the FBI's National Infrastructure Protection Center or the Strategic Information Operations Center were established and ongoing. Unless all indication and warning elements are in place, the Department does not have the assurance that communication channels for sharing vulnerabilities are secure and that components are receiving timely information to better equip it to respond to computer security incidents.⁶

Detailed procedures for the components to follow in reporting computer security incidents were developed by the CSS, but the IMSS could not substantiate whether the procedures were implemented and were being followed by components. According to the IMSS staff, tabulated summaries on the number and type of incidents are reported each month. However, the IMSS could not provide tabulated summaries regarding the nature, frequency, category, and remediation of prior Department computer security incidents or possible trends and potential systemic weaknesses based on analyses of prior incidents. Although there is no specific requirement that the IMSS maintain documentation for these activities, without such documentation the Department does not have assurance that additional procedures for collecting and analyzing incidents as required by the CIP Plan were developed and are in place.

We also found that detailed response procedures for computer security incidents had been established, but the IMSS had not ensured that the procedures were implemented and were being followed. Specifically, the IMSS did not verify whether components had developed, implemented, and maintained internal incident response procedures and whether components had identified appropriate individuals responsible for reporting incidents to the DOJCERT.

Department Order 2640.2D requires components to develop and test contingency plans as well as site plans detailing responses to emergencies

⁶ An incident is an occurrence that has been assessed as having an adverse effect on the security or performance of an information system.

for IT facilities, but the IMSS staff could not provide support that components had done so.

The CIP Task Force was responsible for developing and implementing the CIP Plan, including the emergency management program, but the Task Force ceased operating during calendar year 2000 and has had no further involvement in implementation activities. IMSS officials told the OIG that other activities are operating within the Department to mitigate the activities not performed by the CIP Task Force. As noted previously, we found weaknesses in the Department's emergency management. As a result, the Department has less than adequate assurance that it can effectively respond to computer attacks and security incidents.

Interagency Coordination

There are two primary objectives for establishing effective interagency coordination relating to CIP. First, the CIP Plan requires the Department to establish and maintain effective liaisons with entities proposing and promulgating security measures and plans relating to CIP. Doing so ensures that the Department receives the most up-to-date information for protecting its critical IT asset systems. Second, the CIP Plan requires the Department to establish and maintain effective liaisons with all entities for which Department IT systems either receive or provide critical data supporting national security, national economic security, and/or crucial public health and safety activities. All Department IT systems either receiving or providing such information must be identified and included in the Department's MEI as critical IT assets and receive the special protection afforded under the CIP program.

Although the CIP Plan contained comprehensive requirements for implementing an effective interagency coordination program, as detailed below, such a program has not been established within the Department. IMSS officials did not ensure that components' headquarters and field offices developed lists of current federal and interagency liaisons and memoranda of understanding associated with CIP. The Department did not establish a method for ensuring coordination between the various Department entities and liaisons with outside organizations related to critical infrastructure protection. Components did not forward to the IMSS lists of liaisons and relationships. Consequently, the centralized database of liaisons and relationships was not created and maintained, nor was any entity within the Department serving as the focal point for all liaisons and relationships pertaining to CIP. A working group, or other means of communication, was

not established to ensure that information is effectively shared between Department components having interagency relationships and liaisons.

Without such a program for interagency coordination, the Department cannot ensure that information will be accessible from Department assets when needed.

Resource and Organizational Requirements

The Department's CIP Plan required identification of the resources and organization necessary to protect critical assets. This was to be accomplished largely through the efforts of the CIP Task Force. Although we found that the CIP Task Force did not fully carry out the responsibilities in this area of the CIP Plan, the Department has undertaken some efforts to ensure its resource and organizational requirements are adequately identified. However, full implementation of the CIP Plan has not been achieved. Studies contracted for by JMD done in lieu of studies by the CIP Task Force have not assessed the linkage between budgetary and personnel shortfalls and the Department's critical infrastructure weaknesses. We concluded that completion of this activity is crucial to the Department's efforts to ensure that its resource and organization requirements have been met.

Recruiting, Educating, and Awareness

The Department's 1999 CIP Plan recognized the need to recruit, retain, and educate both Department and contractor personnel in the areas of physical and information security. The Plan called for the completion of various programs to ensure that these needs were met. Some of these programs have been fully accomplished. For example, on April 15, 2003, the Department implemented a departmentwide initiative to provide computer security awareness training. However, we found that the recruitment and retention program called for in the Plan was not fully implemented and, as a consequence, the Department lacks assurance that it has been able to attract and retain the best possible CIP staff.

Follow-up on Prior Audit

In our November 2000 report on "Department Critical Infrastructure Protection – Planning for the Protection of Computer Based Infrastructure," we found that the Department had not yet: 1) identified all of its mission-essential assets, 2) assessed the vulnerabilities of each critical asset, 3) developed remedial action plans for identified vulnerabilities, or

4) developed a multi-year funding plan for reducing vulnerabilities. During this current audit, we tested follow-up actions taken regarding these recommendations. We found that the IMSS had completed some of the required corrective actions. However, further work is required regarding the MEI inventory, plans to address weaknesses identified in vulnerability assessments, and development of a multi-year funding plan for the remediation of vulnerabilities.

Summary

By May 2003 all federal agencies were required to achieve and maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish their ability to perform essential national security missions and ensure general public health and safety. While the Department has activities planned and in-progress to help it reach this full operating capability, some of those plans lack completion dates. Absent those dates, there is no assurance that the Department will ever reach full operating capability. As described above, the Department did not reach full operating capability by May 2003 as required, and as a consequence the Department's critical infrastructures remain at risk.

Recommendations

Our Report contains 26 recommendations to help improve the Department's efforts to manage critical infrastructure protection. These include recommending that the Department:

- develop a risk mitigation tracking system for the inventory of classified mission-essential infrastructure systems;
- develop a multi-year funding plan based on resources required to mitigate vulnerabilities as identified in the Plans of Actions and Milestones;
- develop contingency plans for all critical IT assets;
- test contingency plans periodically as required by Department Order 2640.2D;
- compile a list of links, relationships, and contacts with other federal agencies and other entities (foreign governments, state and local agencies, and the private sector); and

- contact external entities to determine whether any Department assets are critical to their missions.

TABLE OF CONTENTS

BACKGROUND	1
A. The Department's Management of Critical Information Technology Assets	3
B. Framework for Assessing Adequacy of CIP Program...	5
C. Prior Office of the Inspector General Reports	8
D. General Accounting Office Reports	10
FINDINGS AND RECOMMENDATIONS	12
FINDING 1: ESTABLISHING A RISK MITIGATION PROGRAM	12
A. Vulnerability Assessments and Risk Mitigation	12
B. Progress Toward Mitigating Program Vulnerabilities	14
C. Progress Toward Mitigating Critical IT Asset Vulnerabilities	23
D. Conclusions	32
E. Recommendations	33
FINDING 2: ESTABLISHING AN EMERGENCY MANAGEMENT PROGRAM	35
A. Department Efforts to Establish an Emergency Management Program for the Protection of Critical Infrastructure Assets	35
B. Implementation of the Emergency Management Program	37
C. Overall Causes for and Effect of Not Fully Implementing an Emergency Management Plan	46
D. Conclusions	46
E. Recommendations	48
FINDING 3: ESTABLISHING AN EFFECTIVE INTERAGENCY COORDINATION PROGRAM	50
A. Importance of Establishing an Effective Interagency Coordination Program	50
B. CIP Plan Requirements for Establishing an Effective Interagency Coordination Program	51
C. An Interagency Coordination Program as Envisioned in the CIP Plan Was Not Implemented ...	52
D. Reasons Why an Effective Interagency Coordination Program Was Never Established	52

E.	Conclusions	58
F.	Recommendations	59
FINDING 4: MEETING DEPARTMENT RESOURCE AND ORGANIZATIONAL REQUIREMENTS		
		60
A.	Requirement in the CIP Plan	60
B.	Implementation of the CIP Plan for Resource and Organizational Requirements	61
C.	Recommendation	63
FINDING 5: ESTABLISHING EFFECTIVE RECRUITING, EDUCATING AND AWARENESS PROGRAMS.....		
		64
A.	Planned Programs	64
B.	Recruitment	65
C.	Education and Training.....	65
D.	Awareness	66
E.	Recommendation	67
FINDING 6: FOLLOW-UP ON THE PRIOR OIG AUDIT OF DEPARTMENT CRITICAL INFRASTRUCTURE PLANNING FOR THE PROTECTION OF COMPUTER BASED INFRASTRUCTURE		
		68
A.	Inventory the Department's MEI.....	69
B.	Complete Vulnerability Assessments of the Department's MEI by December 31, 2000.....	69
C.	Remedial Plans to Address Weaknesses Identified by the Vulnerability Assessments.....	70
D.	Multi-Year Funding Plan for the Remediation of Vulnerabilities	70
APPENDIX 1	OBJECTIVES, SCOPE, AND METHODOLOGY	71
APPENDIX 2	ABBREVIATIONS AND ACRONYMS.....	73
APPENDIX 3	STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS	75
APPENDIX 4	STATEMENT ON MANAGEMENT CONTROLS.....	76
APPENDIX 5	DEPARTMENT OF JUSTICE'S COMPUTER-BASED MINIMUM ESSENTIAL INFRASTRUCTURES.....	77
APPENDIX 6	CRITICAL ASSET DESCRIPTIONS	78

APPENDIX 7	PCIE/ECIE DESCRIPTION	83
APPENDIX 8	THE TWELVE CRITICAL IT ASSET VULNERABILITIES.....	84
APPENDIX 9	FLOW OF INFORMATION WITH THE DEPARTMENT OF STATE AND US CUSTOMS	90
APPENDIX 10	DEPARTMENT ENTITIES THAT HAD CIP TASK FORCE MEMBERS.....	91
APPENDIX 11	JMD’S RESPONSE TO THE DRAFT REPORT	92
APPENDIX 12	OIG, AUDIT DIVISION ANALYSES AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT	101

BACKGROUND

According to the July 2002 Office of Homeland Security's, "National Strategy for Homeland Security," terrorists may seek to cause widespread disruption and damage, including casualties, by attacking electronic and computer networks which are linked to other critical infrastructures. Terrorist groups exploit new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely. Cyber attacks are anticipated to become an increasingly significant threat as terrorists further develop their technical capabilities and become more familiar with potential targets.

The February 2003 Office of Homeland Security's National Strategy to Secure Cyberspace indicates that a spectrum of malicious actors can and do conduct attacks against our critical information infrastructures.⁷ Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to the nation's critical infrastructures, economy, or national security. The required technical sophistication to carry out such an attack is high and partially explains the lack of a debilitating attack to date. However, there have been instances where attackers have exploited vulnerabilities that may be indicative of more destructive capabilities.

According to the National Plan for Information Systems Protection, the threat is that a group or nation hostile to the United States will seek to "inflict economic damage, disruption and death, and degradation of our defense response" by attacking our critical infrastructure. Presidential Decision Directive 63 (PDD 63) requires that the Department of Justice's (Department) critical infrastructure protection plans include an inventory of the Department's mission-essential assets, an assessment of each asset's vulnerabilities, and plans to remediate those vulnerabilities.

The terrorist attacks of September 11, 2001, prompted the Attorney General to make counterterrorism the Department's highest priority. The Department reflected this new priority in its Strategic Plan for Fiscal Years 2001 – 2006, which was issued in November 2001. In the Strategic Plan, the Attorney General recognized that in the fight against terrorism, the Department would need to improve the integrity and security of computer systems and make more effective use of information technology.

⁷ On March 1, 2003, the Department of Homeland Security (DHS) was created, and all of the functions and duties of the Office of Homeland Security were transferred to it. The National Strategy to Secure Cyberspace is an implementing component of the National Strategy of Homeland Security.

PDD 63 issued in May 1998 called for a national effort to assure the security of the nation's critical infrastructure. The critical infrastructure consists of physical and computer-based systems essential to the minimum operations of the economy and government. This includes, but is not limited to telecommunications, banking and finance, energy, transportation, and essential government services. The minimum essential infrastructure (MEI) is the framework of critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes essential to accomplishing an organization's core mission as they relate to national security, national economic security, or continuity of government services.

PDD 63 requires that agencies take measures to eliminate any significant vulnerability to both physical and cyber attacks on the nation's critical infrastructures. Each federal department and agency was required to prepare a plan for protecting its own critical infrastructure, including an inventory of the department's or agency's mission-essential assets and an assessment of the vulnerabilities of those essential assets.

Under PDD 63, by December 2000 departments and agencies were to have assessed information system vulnerabilities and adopted a multi-year funding plan to remedy the vulnerabilities. By May 2003, departments and agencies were to have achieved "full operating capability." The National Plan for Information Systems Protection, Version 1.0, issued by the Critical Infrastructure Assurance Office (CIAO), describes full operating capability as the ability to ensure that any interruption or manipulation of critical functions is "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States." The Draft Critical Infrastructure Protection (CIP) Plan indicates that full operating capability for the Department is comprised of:

- identifying the MEI, interdependencies, vulnerabilities, and developing plans to address the vulnerabilities;
- detecting attacks and unauthorized intrusions;
- sharing attack warning and information in a secure and timely manner; and
- responding to attacks, and reconstituting and recovering assets that were subject to attacks.

A. The Department's Management of Critical Information Technology Assets

The Justice Management Division (JMD) develops, promulgates, and reviews implementation of departmentwide policies, standards, and procedures for the management of automated information processing resources. Within JMD, the Chief Information Officer (CIO) has oversight responsibility for the implementation of CIP within the Department. Within the Office of the CIO, the Information Technology Security Staff (ITSS) has primary responsibility for critical infrastructure planning and implementation.⁸

The ITSS was established within the Office of the CIO in May 2003, and its 14-member staff is responsible for developing and implementing policies and procedures for IT investment management and information systems security programs. Prior to May 2003 the responsibilities now managed by the ITSS were managed by the IMSS. With the change of name in May 2003, the ITSS retained the prior staff of the IMSS and the prior IMSS's responsibilities for oversight of the CIP program. In addition, the ITSS gained responsibility from JMD Computer Services Staff (CSS) for managing the Department of Justice Computer Emergency Response Team (DOJCERT). The DOJCERT assists component organizations with incident handling and resolution, and it is the centralized reporting entity for the Department. All components are required to report incidents to the DOJCERT. The DOJCERT issues any necessary alerts to components and external agencies.

Within the Department, critical infrastructure protection is a shared responsibility among JMD and various component organizations. Each component aids the IMSS in identifying its MEI, developing remediation and funding plans, and ensuring the implementation of the plans. JMD is responsible for coordinating the departmentwide effort and ensuring that the components comply with applicable requirements.

In our November 2000 report on "Department Critical Infrastructure Protection – Planning for the Protection of Computer Based Infrastructure," we stated that as required by PDD 63, JMD submitted the Department's

⁸ Prior to September 11, 2002, JMD Security and Emergency Planning Staff (SEPS) had oversight for information technology (IT) security for the classified systems of the Department and Information Management and Security Staff (IMSS) had oversight for the sensitive but unclassified (SBU) systems. Since that time, the CIO is responsible for overseeing and implementing security policy and practices for both National Security Information (NSI) and SBU systems. The standards, procedures, and guidelines are coordinated with the Department's Security Officer.

initial critical infrastructure plan to the CIAO in November 1998 (November 1998 Plan). In January 1999, the Expert Review Team returned the results of its review and asked the Department to revise the plan accordingly.⁹ The Department addressed some of the Expert Review Team's comments and submitted its revised plan to the CIAO in April 1999.

In response to the Department's new priorities following September 11, 2001, JMD made changes in its strategic priorities and business practices. Among these changes, JMD issued guidance that there would be an equal emphasis on the protection of critical assets, whether physical, personnel, or cyber-based. A revalidated MEI was completed December 2002. The revalidation process incorporated the change in emphasis on physical assets and personnel, a 72-hour loss criteria developed by the CIAO, and changes in the goals and strategic objectives in the Department's Strategic Plan.

The Department's MEI has evolved over time as a result of policy changes and JMD's refinement of its inventory of critical assets. The December 2002 version of the MEI consists of 21 systems from three Department components – the Drug Enforcement Agency (DEA), Federal Bureau of Investigation (FBI), and JMD. By contrast, the January 2001 version of the MEI consisted of 20 systems from those same components and the Immigration and Naturalization Service (INS). Both inventories are contained in Appendix 5 of this report. When the MEI was revalidated in December 2002, eight assets were removed from the January 2001 version, and nine others were added. During the period of our review, the IMSS, at various times, had CIP oversight responsibilities for 29 critical assets.¹⁰

⁹ PDD 63 created an interagency Expert Review Team. The Expert Review Team reviewed and commented on agency plans in accordance with a set of essential plan elements to ensure quality, continuity, and effective implementation of agency plans to protect critical infrastructures.

¹⁰ During the course of our audit, the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) joined the Department of Justice and the INS transferred to the DHS. The CIP efforts that we evaluated did not include any CIP efforts associated with the ATF, except as noted on page 23.

B. Framework for Assessing Adequacy of CIP Program

In 1999 the President's Council on Integrity and Efficiency (PCIE) initiated a governmentwide review of the nation's critical infrastructure assurance program.¹¹ The review is being completed in four phases. The objective of the Phase 1 review was to assess the adequacy of the agency planning and assessment activities for protecting critical cyber-based infrastructures. The objective of Phase 2 was to assess the adequacy of agency implementation activities for protecting their critical cyber-based infrastructure. In Phase 3 we assessed the adequacy of agency planning and assessment activities for protecting the Department's critical noncyber-based infrastructures. The objective of Phase 4 will be to assess the adequacy of implementation activities for protecting noncyber-based infrastructures. In the Department, we previously completed audits for Phases 1 and 3.¹² This audit is performed as part of Phase 2 of the PCIE effort.

During Phase 1, we reviewed the adequacy of Department plans, asset identification efforts, and initial vulnerability assessments. Over 20 Inspectors General conducted similar audits in their own agencies as part of an effort sponsored by the PCIE. The Phase 1 report, issued November 2000, stated that the Department had submitted its initial critical infrastructure protection plan to the CIAO as required. The Phase 1 report also stated that the Department revised its initial plan according to comments received from an Expert Review Team.

Our Phase 1 audit assessed the Department's compliance with the following requirements:

- development of a CIP Plan;
- Expert Review Team Review;
- appointment of a Chief Infrastructure Assurance Officer;
- identification of cyber-based MEI;

¹¹ The PCIE, comprising all Presidentially-appointed Inspectors General, coordinates interagency and intra-entity audit, inspections, and investigations dealing with governmentwide issues of waste, fraud, and abuse. See Appendix 7 for more details on the PCIE.

¹² The PCIE/ECIE (Executive Council on Integrity and Efficiency) delayed the Phase 2 Review until after Phase 3 to allow agencies sufficient time to implement their CIP programs.

- vulnerability assessments;
- risk mitigation plans to stem potential damage from each vulnerability;
- establishment of an emergency management program;
- incorporation of critical infrastructure into strategic planning and the performance measurement framework;
- identification of resource and organizational requirements;
- development of a program to ensure that the Department has the personnel and skills necessary to implement a sound infrastructure protection program; and
- establishment of effective CIP coordination with other applicable entities (foreign, state and local governments, and private industry).

Asset identification efforts are the Department's measures employed to identify its MEI. The Department's CIP Plan indicated that the methodology to identify its MEI was to create a rank-ordered list of assets including a brief description of the asset, location, specific mission-based criteria used to identify the asset, estimated replacement costs, planned life cycle, and a brief statement as to the potential impact of the asset not being available.

A vulnerability assessment is a systematic examination of the ability of a system or application, including current security procedures and controls, to withstand assault. Agencies use vulnerability assessments to identify weaknesses that could be exploited and to predict the effectiveness of additional security measures in protecting critical assets from attack. The outcome of the assessment is a list of flaws or omissions in controls that may affect the integrity, confidentiality, accountability, and availability of resources that are essential to critical assets.

In Phase 2 of the governmentwide PCIE review, the subject of this report, we audited the adequacy of implementation activities for protecting critical cyber-based infrastructures. Specifically, we assessed the adequacy of agency activities in the following areas: 1) risk mitigation; 2) emergency management; 3) interagency coordination; 4) resource and organizational requirements; and 5) recruitment, education, and awareness.

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management. Risk mitigation follows the Department's identification of critical assets and performance of

a vulnerability assessment that identifies weaknesses that could be exploited.

The goal of the emergency management program is to minimize the known vulnerabilities associated with the most critical asset and infrastructure dependencies in an expeditious and cost-effective manner, and to permit the operations of critical functions in the event of disruptions. The emergency management program should include such items as indications and warnings (of an attack), incident collection, reporting and analysis, response and continuity-of-operation plans, and plans to reconstitute minimum required capabilities following a successful attack.

Interagency coordination is important because many federal government programs rely on the resources of other government agencies to fulfill their missions. Because of such reliance, the Department should identify and characterize the level to which Department assets provide support to other government agencies. Additionally, it is necessary to identify liaisons, and the nature of the coordination link between the entities.

Recruitment refers to the Department's efforts to acquire highly skilled information technology (IT) security personnel to implement the CIP program. Education, training, and awareness are also necessary to the successful implementation of any information security program. These three elements are related, but the elements involve distinctly different levels of learning. Training is geared to understanding the security aspects of the particular IT systems and applications that the individual uses. Education differs from training in both breadth and depth of knowledge and skills acquired. Security education, including formal courses and certification programs, is most appropriate for an organization's designated security specialists. Awareness is not training but is a prerequisite to it. The purpose of an awareness program is to focus attention on security. Awareness provides a baseline of security knowledge for all users, regardless of job duties or position.

In our Phase 3 report, issued November 2001, we reviewed the adequacy of the Department's planning and assessment activities for protecting its critical noncyber-based infrastructures. Specifically, we assessed the adequacy of agency plans, asset identification efforts, and initial vulnerability assessments of personnel and physical assets. The report indicated that the Department had not yet: 1) adequately identified all of its mission essential assets, 2) assessed the vulnerabilities of each of its systems, 3) developed remedial action plans for identified vulnerabilities, and 4) developed a multi-year funding plan for reducing vulnerabilities.

Phase 4, if pursued, will target the adequacy of implementation activities for protecting critical noncyber-based infrastructures. Specifically,

it will review the adequacy of agency activities in the following areas: risk mitigation; emergency management; interagency coordination; resource and organizational requirements; and recruitment, education and awareness.

C. Prior Office of the Inspector General Reports

We have recently performed two types of audits relevant to the Department's management of critical infrastructure. These audits are: 1) program audits of JMD's CIP management efforts and 2) computer security audits performed pursuant to the Government Information Security Reform Act (GISRA).¹³

1. Program Audits

In our November 2000 report on "Department Critical Infrastructure Protection – Planning for the Protection of Computer Based Infrastructure," we found that the Department had not yet: 1) identified adequately all of its mission-essential assets, 2) assessed the vulnerabilities of each critical asset, 3) developed remedial action plans for identified vulnerabilities, and 4) developed a multi-year funding plan for reducing vulnerabilities. As a result, the Department's ability to perform certain vital missions was at risk from terrorist attacks or similar threats.

Specifically, the Department's identification of mission-essential assets did not meet the intent of PDD 63 because it did not include personnel, interdependencies, and a complete list of facilities. Further, the methodology used did not link the MEI to those Department missions absolutely necessary to national security, national economic security, or the continuity of government services, and it did not document the criteria used to select each asset.

Additionally, in our November 2000 report, we noted that the Department decided not to fund an adequate vulnerability assessment. The vulnerability assessment included in a draft plan differed from the assessment plan in the previous version. The draft plan was based on a framework sponsored by the CIAO and reviewed by the Expert Review Team, two organizations outside of the Department with responsibility for implementing PDD 63. The revised vulnerability assessment was based on a review of past audits, compliance reviews, and assessments. As a result, the Department had not developed an inventory of flaws or omissions in

¹³ Beginning in November 2000, GISRA required the Office of the Inspector General (OIG) to perform independent evaluations of the Department's information security program and practices. Beginning in FY 2003, these audits are now being conducted under the provisions of Federal Information Security Management Act of 2002.

controls (vulnerabilities) that may affect the integrity, confidentiality, accountability, and availability of resources that are essential to critical assets.¹⁴ Department officials said that vulnerability assessments would be performed as part of a certification and accreditation (C&A) process as ordered by the Assistant Attorney General for Administration.¹⁵

In our November 2001 report on "Department Critical Infrastructure Protection – Planning for the Protection of Physical Infrastructure," we found that the Department had not yet: 1) adequately identified its physical MEI, 2) ensured that complete vulnerability assessments of all of its physical mission-essential assets have been performed, 3) developed plans to remediate weaknesses identified in the vulnerability assessments of its physical MEI, and 4) developed a multi-year funding plan for reducing vulnerabilities. While the Department initially disagreed with the results of this audit, in May 2003 JMD agreed to carry out the recommended corrective action.

2. GISRA Audits¹⁶

For FY 2001, we audited the security of four classified and five SBU computer systems. We issued two separate reports consolidating our results, one for unclassified systems and one for classified systems.¹⁷ The report on SBU systems was issued without recommendations. Both reports stated that the Department did not adequately:

- identify and assess risks to determine needed security measures,

¹⁴ In Finding 6 of this report, we provide an assessment of JMD's corrective actions with regard to the findings of our November 2000 report.

¹⁵ Certification consists of a technical evaluation of a sensitive application to see how well it meets security requirements. Accreditation is the official management authorization for the operation of the application and is based on the certification process as well as other management considerations.

¹⁶ In fulfilling its FY 2002 GISRA review requirements, the OIG reported on both classified and SBU systems in its "Independent Evaluation Pursuant to the Government Information Security Reform Act Fiscal Year 2002 Consolidated Report," Report Number 03-19. The report is a classified document and has not been released publicly.

¹⁷ The report for the unclassified systems is "Summary of the Independent Evaluation Pursuant to the Government Information Security Reform Act, Fiscal Year 2001 Sensitive But Unclassified Systems," Report Number 02-18. The report for the classified systems is "Summary of the Independent Evaluation Pursuant to the Government Information Security Reform Act, Fiscal Year 2001 Classified Systems," Report Number 02-21.

- establish and implement policies and controls to meet those needs,
- promote awareness so that users understand the risks and the related policies and controls required to mitigate them, or
- monitor and evaluate established policies and controls to ensure that the policies and procedures were both appropriate and effective.

Three of the five SBU systems tested had one or more of the following vulnerabilities related to contingency planning.

- Restoration priorities were not identified and an interagency agreement did not exist for the alternative processing site.
- Contingency plans were not properly reviewed or approved.
- Contingency plans were not tested.
- Contingency plan training was not conducted.

D. General Accounting Office Reports

The General Accounting Office (GAO) has conducted several reviews of CIP-related efforts within the government. The following reports are among its most recent in areas related to CIP.

In a January 2003 report titled "Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures" (GAO-03-121), the GAO noted cyber CIP as a high-risk area because, in part, terrorist groups and others have stated their intentions of attacking critical infrastructures. Failure to adequately protect these infrastructures could adversely affect national security, economic security, and/or public health and safety. The GAO acknowledged that improvements are underway. The GAO reported that recent audits of 24 of the largest agencies continue to identify significant information security weaknesses that put critical federal operations and assets in each of these agencies at risk.

In an October 2001 report titled "Information Sharing – Practices that Can Benefit Critical Infrastructure Protection" (GAO-02-24), the GAO noted that information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to combating computer-based threats. The GAO indicated that trust is the essential underlying element to successful information-sharing relationships. The GAO identified three other critical factors for successful information-sharing relationships:

- establishing effective and appropriately secure communication mechanisms (such as regular meetings and secure websites),
- obtaining support of senior managers at member organizations regarding the sharing of potentially sensitive member information and the commitment of resources, and
- ensuring organization leadership continuity.

The GAO noted that one of the most difficult challenges was overcoming organizations' initial reluctance to share information. Other challenges included: 1) developing agreements on the use and protection of shared information, 2) obtaining adequate funding to cover the cost of items such as websites and meetings while avoiding seeking contributions intended primarily to promote the interests of an individual organization, 3) maintaining a focus on emerging issues of interest to members, and 4) maintaining professional and administrative staff with appropriate skills.

FINDINGS AND RECOMMENDATIONS

1. ESTABLISHING A RISK MITIGATION PROGRAM

Our audit found that the IMSS had not established an effective risk mitigation program.¹⁸ Regarding identified CIP program vulnerabilities, IMSS staff indicated that mitigation actions were progressing on schedule; however, we found that the IMSS did not effectively manage the mitigation actions in that project plans lacked key milestone dates and the IMSS did not provide components sufficient time to provide required data for the revalidation of the MEI. Regarding the mitigation of critical IT system vulnerabilities, we found that progress plans to ensure correction of identified security weaknesses were not adequately prepared by the components to allow effective monitoring by the IMSS. This problem occurred because of the short time given to the components to respond and because the components did not adequately respond to data requested by the IMSS for mitigation plans. As a result, the Department has less than adequate assurance that critical IT asset vulnerabilities will be mitigated adequately or timely.

A. Vulnerability Assessments and Risk Mitigation

The purpose of the vulnerability assessment is to provide the Department's Chief Infrastructure Assurance Officer with an overall assessment of the CIP program and the vulnerabilities associated with its critical IT system assets.¹⁹ The Department's critical IT assets as they relate to CIP are also referred to as the Department's MEI.

The vulnerability assessment identifies the risks and vulnerabilities to the Department's CIP program and its MEI systems and makes recommendations to mitigate the identified risks. In addition, the funding level associated with IT security for each MEI asset and the overall program funding level are identified. This allows the Department's CIO to make informed decisions in support of the Department's ability to execute its

¹⁸ In May 2003, the CIO reorganized the information resource management function of the Office of the Chief Information Officer. The IMSS was renamed the Information Technology Security Staff (ITSS).

¹⁹ The Chief Infrastructure Assurance Officer is responsible for the protection of all aspects of that department's critical infrastructure other than information assurance. The CIO is responsible for information assurance. PDD 63 requires these officials to establish procedures for obtaining expedient and valid authorities to allow vulnerability assessments to be performed on government computer and physical systems.

mission and goals as those decisions relate to critical infrastructure protection.

Upon completion of the vulnerability assessment, the Department components develop remedial action plans to mitigate the exploitation and the impact of any identified vulnerabilities against critical infrastructure assets until such time as the vulnerability can either be eliminated or reduced to an acceptable level. Remediation refers to those precautionary actions taken before undesirable events occur to reduce known deficiencies and weaknesses that could cause an outage or compromise a law enforcement infrastructure sector or critical asset. The precautions are applicable regardless of whether those events are acts of nature, technology, or through malicious intent. Remediation may include education and awareness, operational process or procedural change, system configuration changes, or system component changes.

The remedial action plan should be system specific and at a minimum contain the following information:

- responsible office,
- identification of vulnerability,
- mission impact,
- mitigation action,
- long-term correction, and
- estimated cost and milestones for recommended corrective measures.

Initially, a CIP Task Force was scheduled to complete the Department Vulnerability Assessment by December 30, 1999, with approval by the Chief Infrastructure Assurance Officer on January 7, 2000.²⁰ The IMSS staff could not explain why the CIP Task Force stopped convening during calendar year 2000, and the Task Force took no further action to complete the vulnerability assessments. JMD eventually completed the assessment in March 2002. The completed vulnerability assessment identified a total of 16 vulnerabilities, 4 of which pertained to the Department's overall CIP program, while the remaining 12 addressed risks in the 20 information

²⁰ The Department's April 1999 CIP Plan provided that "A Critical Infrastructure Protection Task Force (CIPTF) will be responsible for CIP Plan development and implementation within their respective components" The CIP Task Force was comprised of representatives from law enforcement, litigating divisions, and administrative offices. See Appendix 10 for a list of points of contact for the CIPTF.

technology systems identified in the Department's January 2001 MEI. For individual vulnerabilities, an associated risk rating and the mitigating action for eliminating the vulnerability or reducing the risk of the vulnerability to an acceptable level were identified.

Our audit work disclosed that the IMSS did not establish an effective Department risk mitigation program and that the IMSS's efforts to monitor mitigation actions were not effective. As a result, critical IT asset vulnerabilities may not be adequately or timely mitigated. The specific program and IT asset risk mitigation deficiencies we identified are discussed in the report sections that follow.

B. Progress Toward Mitigating Program Vulnerabilities

JMD completed a vulnerability assessment in March 2002. JMD reviewed the management controls developed to implement the Department's CIP program and evaluated the controls against requirements contained in reports and other documents from the GAO, the National Critical Infrastructure Assurance Office, and the General Services Administration (GSA). The JMD review identified four individual vulnerabilities associated with the program. The vulnerabilities are listed below and discussed in greater detail beginning in the following text.

1. The CIP Plan was out of date and needed to be updated to incorporate the implementation plan and the Department's new Strategic Plan.
2. The inventory of mission-essential assets required revalidation by components after the events of September 11, 2001.
3. JMD needed to address the risk of not meeting the full operating capability date of May 2003.
4. Seven of the mission-essential systems required an independent evaluation.

Several items remain to be completed before the Department can reach full operating capability. In July 2002, IMSS officials indicated that mitigation action for all program vulnerabilities was progressing on target and would be completed on schedule. Our audit work initially found that the IMSS did not effectively manage the mitigation actions. Specifically, project plans were not developed and followed, and the IMSS did not provide components sufficient time to provide required data for the revalidation of the MEI.

We assessed the April 2003 draft CIP plan for project plans. We found that while the IMSS/ITSS had completed project plans, those plans did not include milestone dates by which tasks were to be completed. Those plans did not include completion dates for all tasks, and 54 of 73 tasks were not completed by May 2003. However, in our judgment four key tasks prevent the Department from achieving full operating capability. The four tasks are:

- development of contingency plans for systems without plans or revision of inadequate plans (discussed in further detail in finding 2),
- testing of the contingency plans (discussed in further detail in finding 2),
- incorporation of vulnerabilities into the Security Management and Report Tool (SMART) database for tracking purposes (discussed later within this finding),²¹ and
- development of a SMART database for classified systems (discussed later within this finding).

(1) Program Vulnerability #1: Outdated CIP Plan

The March 2002 Vulnerability Assessment discussed the outdated CIP Plan as follows.

Vulnerability:	The CIP Plan is out of date and needs to be updated to incorporate the implementation plan and the Department's new Strategic Plan.
Threat:	All threats could exploit this vulnerability.
Discussion:	The current plan is over two years old and does not contain current information on the implementation of the Department's protection strategy. PDD 63 requires CIP Plans to be updated at least every two years. Justice Management Division has an informal implementation [plan] for the next phases of the protection strategy, but has not incorporated this plan into the overall Department CIP Plan.
Risk Rating:	Low – Moderate
Mitigation Action:	JMD will update the CIP Plan and will ensure it is in compliance with the new Executive Orders and other Federal guidance on CIP. In addition, the Plan will map the MEI assets to the Department's new Strategic Plan. Estimated completion: December 2002

Source: Justice Management Division's March 2002 Vulnerability Assessment

²¹ The SMART database is a set of user interface, database management, and business intelligence tools designed to assist the Department CIO and program managers as well as the security administrators in identifying, controlling, and monitoring the performance of a component IT security program and its systems.

The Department's CIP Plan presents the broad direction for the Department's critical infrastructure assurance and provides the longer-range goals, strategies, and performance indicators by which to measure progress toward implementing a viable CIP program. Intended as a "living document," the CIP Plan provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the Department's physical and cyber security controls. The Department's initial CIP Plan was prepared by JMD in November 1998. The Plan was revised in April 1999 to address comments of prior reviews of the CIP program.

The March 2002 Vulnerability Assessment identified that the CIP Plan needed updating to incorporate the next phases of the protection strategy and the Department's new strategic plan. The IMSS staff informed us that the task of updating the Plan was assigned to a contractor. The contractor serves as an information technology security consultant to JMD and senior Department managers. Some of the tasks performed by the contractor relating to the Department's vulnerability assessment include providing general IT support to the IMSS, developing a comprehensive vulnerability assessment methodology, and researching and reporting on various methods of performing follow-up actions to ensure vulnerabilities or other issues identified during the performance of vulnerability assessments have been corrected. The contractor also performs other duties not related to the vulnerability assessment such as assisting in data entry for the SMART database.

According to the March 2002 Vulnerability Assessment, the estimated completion date for updating the Plan was December 2002. A Draft CIP Plan was completed April 21, 2003, and finalization was pending comments requested on the plan from the Department of Homeland Security (DHS). IMSS officials indicated that they delayed completion of the new CIP Plan to incorporate guidance from the DHS's most recent draft of the National Strategy to Secure Cyberspace.

(2) Program Vulnerability #2: Revalidating MEI Assets after Events of September 11, 2001

The March 2002 Vulnerability Assessment discussed revalidating MEI assets as follows.

Vulnerability:	MEI assets should be revalidated after the events of September 11, 2001.
Threat:	All threats could exploit this vulnerability.
Discussion:	The Department's MEI assets were determined prior to the events of September 11, 2001. Although the Department did use the methodology as defined by the CIAO's office, the Department should revalidate the MEI inventory with the components and program managers to ensure all MEI assets are included and meet the CIAO's revised requirements. As an example, the CIAO introduced a 72-hour time requirement on the availability of an IT system; the system is not considered critical unless it's non-availability for 72 hours will prevent the Department from fulfilling its PDD 63 missions. Additionally, the INS and FBI have identified additional systems during the C&A process that have not been assessed relating to CIP activities.
Risk Rating:	Moderate
Mitigation Action:	JMD will explore the use of Project Matrix to assist the Department in revalidating the MEI systems and critical assets. ²² If Project Matrix is not used, JMD, using contractor support, will revalidate the Department's MEI IT assets. Justice Management Division will use the same approved methodology for the revalidation as was used for the initial selection of MEI along with new guidance identified by the CIAO's office. Estimated completion: November 2002

Source: Justice Management Division's March 2002 Vulnerability Assessment

Crucial to developing and implementing a CIP Plan is the identification of critical infrastructure assets. Within the Department, the critical infrastructure is comprised of the computer systems, physical assets, and personnel necessary for the Department to carry out its law enforcement and counterterrorism duties. In identifying the Department's critical computer systems, the CIP Task Force focused on internal and external critical infrastructure components that are needed to protect or support safety and health, law enforcement and national security, the Department's litigation function, the administration of justice, and the Department's business functions. Once the Department's critical infrastructure assets were identified, the assets were listed in a consolidated MEI inventory.

²² Project Matrix is the name given to a method developed by the CIAO to assist federal civilian departments and agencies to accomplish identification of critical functions and services and the assets and links necessary to perform that identification. Project Matrix provides an objective process to make the determination of national criticality by performing standardized, systematic evaluation of an organization's functions and services and giving each a criticality score.

The Department's MEI inventory was identified in a joint effort between the components, SEPS, and IMSS using criteria based on guidance from the CIAO. The identification of the Department's minimum essential infrastructure was completed and formally approved by the Assistant Attorney General for Administration on January 16, 2001. The completed inventory is comprised of three sections: 1) critical IT assets, 2) critical physical assets, and 3) critical personnel assets. Prior to the INS transfer to the DHS in March 2003, the MEI included 20 systems in the DEA, FBI, INS, and JMD.

Subsequent to the events of September 11, 2001, some requirements for critical systems have been revised, and two components (the FBI and INS) have identified additional systems that have not been assessed relative to CIP activities. In view of these developments, JMD identified this as a program vulnerability in its March 2002 Vulnerability Assessment.

According to the March 2002 Vulnerability Assessment, the estimated completion date for revalidating MEI assets was November 2002. The IMSS staff indicated that progress toward the completion date was satisfactory, and that components had a November 1, 2002, suspense date for submitting their updated MEIs to JMD. On October 7, 2002, we asked the IMSS staff for a copy of the memorandum to the components establishing the November 1, 2002, suspense date. The Assistant Director of IMSS responded by saying that the memorandum had not been sent and that the draft was still on his desk. According to the contractor status reports, the contractor had completed the draft by August 12, 2002. The IMSS staff said the memorandum hadn't been mailed because of a shortage of staff. Although the memorandum was eventually sent to the components on October 11, 2002, this was hardly sufficient time for the components to update their MEIs and respond by the November 1, 2002, suspense date.

The revalidated MEI was completed in December 2002. Both the old and new MEI are contained in Appendix 5 of this report. Eight assets were removed from the January 2001 MEI and an additional nine assets were added. A description of the MEI assets is contained in Appendix 6. The assets removed from the MEI were:

INS – Central Index System (CIS)
Enforcement Case Tracking System (ENFORCE)
Automated Biometric Identification System (IDENT)
Immigration and Naturalization Service's
Integrated National Communications System (INSINC)

FBI – Criminal Justice Information System Wide Area Network
(CJIS WAN)
InfraGard
Intelligence Information System Network (IISNET)
Secure Automated Messaging Network (SAMNET)

The INS assets were removed in anticipation of the transfer of the INS to the DHS. The FBI assets were removed based on a determination that the loss of those assets for 72 hours would not impede the Department from performing its critical infrastructure protection duties.

The assets added to the MEI were:

DEA – Centralized Data Intercept
Electronic File Room
Wide Area Network
GESCAN
Firebird nodes in Special Operations Division
(SOD) and Command Center

FBI – Key Asset Database
Secure Radio System
Digital Storm Collection

JMD – Metropolitan Area Network (MAN)

These assets were added to the MEI based on the revised requirements for identifying critical systems.

(3) Program Vulnerability #3: Risk of Not Meeting Full Operating Capability by May 2003.

The March 2002 Vulnerability Assessment discussed the risk of not meeting full operating capability as follows.

Vulnerability:	Risk of not meeting the Full Operating Capability date of May 2003.
Threat:	All threats could exploit this vulnerability.
Discussion:	PDD 63 requires that by May 2003 all Federal agencies achieve and maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish its abilities to perform essential national security missions and ensure general public health and safety. This is referred to as "full operating capability" in PDD 63. Any interruptions of these functions must be brief, infrequent, manageable, and minimally detrimental to the welfare of the United States. To achieve the full operating capability, the Department needs to be able to participate in information/intelligence sharing, respond to attacks, or reconstitute systems after successful attacks.
Risk Rating:	Moderate
Mitigation Action:	JMD will Coordinate with the Department's computer emergency response team and components with MEI systems to ensure they have coordinated actions in the event of an attack. Justice Management Division will also coordinate with the components to ensure the contingency plans for critical IT assets are tested and kept up to date. The Department must address the vulnerabilities identified within the individual MEI system assets, and prioritize the vulnerabilities with greatest risks to the Department. Estimated completion: May 2003

Source: Justice Management Division's March 2002 Vulnerability Assessment

By May 2003 all federal agencies were to achieve and maintain "full operating capability" to protect our nation's critical infrastructures from intentional acts that would significantly diminish its abilities to perform essential national security missions and ensure general public health and safety. According to the Department's March 2002 Vulnerability Assessment, the estimated completion date for achieving full operating capability was the same as the deadline identified in PDD 63, May 2003.

Officials of the IMSS indicated that there are four main aspects to attaining full operating capability:

- relocating the DOJCERT to the newly established ITSS,
- integrating the Department's CIP Plan with the planning efforts of the National Infrastructure Protection Center (NIPC),²³
- increasing the reporting of incidents of infrastructure attacks (as of October 2002, only the FBI reported incidents involving SBU systems), and

²³ The National Infrastructure Protection Center serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.

- completing an update to the CIP Plan.

The National Plan for Information Systems Protection, Version 1.0, issued by the CIAO, describes full operating capability as the ability to ensure that any interruption or manipulation of critical functions is “brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.” The Draft CIP Plan indicates that full operating capability for the Department is comprised of:

- identifying the MEI and interdependencies and identifying and addressing their vulnerabilities,
- detecting attacks and unauthorized intrusions,
- sharing attack warning and information in a secure and timely manner, and
- responding to attacks and reconstituting and recovering assets that were subject to attacks.

In April and May 2003, we sought to update the Department’s status in achieving full operating capability. In addressing vulnerabilities identified for the MEI, we noted that the incorporation of vulnerabilities into the SMART database for tracking purposes was incomplete since the database was not set up to track vulnerabilities for classified systems. In assessing the Department’s ability to reconstitute and recover assets after an attack, we noted that there were no dates provided for the development of contingency plans for components without plans nor were dates provided for the revision of inadequate plans. Additionally, no further guidance was provided to require testing of the contingency plans. Generally, the IMSS staff could not provide the status of this effort, schedules, or milestone dates for completing the effort.

The Department did not reach full operating capability by May 2003 as required. However, the Department has activities planned and in progress to help it reach full operating capability. Some of those plans lack dates for completion. Absent those dates, there is no assurance that the Department will complete those activities timely or reach full operating capability.

(4) Program Vulnerability #4: Seven MEI Systems Have Not Been Independently Evaluated

The March 2002 Vulnerability Assessment discussed independent evaluation of MEI systems as follows.

Vulnerability:	Seven of the MEI systems have not been independently evaluated and contain unknown system vulnerabilities.
Threat:	All threats could exploit this vulnerability.
Discussion:	Of the 20 MEI systems, 7 have not received an independent evaluation. The current assessments rely only on the program manager's assessment.
Risk Rating:	Low
Mitigation Action:	JMD will conduct IV&V [independent verification and validation] or penetration testing for the systems that have not undergone any independent evaluation. Two of the FBI systems (SAMNET and InfraGard) will be evaluated by the FBI later this year [2002]. Three systems [DEA Model 204 (M204), Integrated Automated Fingerprint ID System (IAFIS), and National Crime Information Center System, (NCIC 2000)] are currently undergoing IV&V, and the final two systems (ENFORCE, IDENT) will be scheduled for review in late 2002 along with the two FBI systems. Estimated completion date: January 2003

Source: Justice Management Division's March 2002 Vulnerability Assessment

Department of Justice Order 2640.2D requires components to ensure the C&A of all systems under their operational control prior to being placed into operation. Until an IT system is certified and accredited, no operational data can be used for any purpose, including testing in pilot systems if live data is used or if the pilot system is connected to a Department network.

For each classified system and for each SBU system the C&A includes:

- preparing a system security plan;
- performing a risk analysis to identify security risks, determine their magnitude, and identify areas needing safeguarding;
- conducting and documenting a system test and evaluation;
- developing a security procedures guide;
- preparing and testing a contingency plan;
- preparing a summary of compliance with the security requirements and the statement of residual risk; and
- preparing a security evaluation report with a recommendation as to whether or not to accredit the system based on documented residual risks.

Once a Department component completes the C&A and its documentation, the C&A is submitted to JMD for the IV&V process that is contracted out to one of four contractors.

The March 2002 Vulnerability Assessment identified that of the 20 mission-essential information systems in the Department, 7 had not received an IV&V as part of the C&A process. We found that the accuracy of IMSS's documented support of its monitoring efforts was questionable. An initial status was documented in the March 2002 Vulnerability Assessment, and again in an undated document that we were told was prepared in October 2002. In the March 2002 Vulnerability Assessment, the FBI's IAFIS and NCIC 2000 systems were both reported as undergoing IV&V process; however, in the previously mentioned undated document, both systems were reported as still undergoing the initial certification and accreditation by the FBI's Security Division. As of May 2003, IAFIS and NCIC 2000 had not undergone the IV&V process. Independent Verification and Validation is a requirement of the certification and accreditation process.

Further, the ATF transferred to the Department from the Department of Treasury in January 2003. According to IMSS staff, ATF systems had received interim certification, and full certification and accreditation of these systems was expected to be completed by September 30, 2003. Critical assets from the ATF had yet to be identified. As a consequence, a vulnerability assessment, risk mitigation plans, and multi-year funding plans had not been developed for critical assets of the ATF.

Information Management and Security Staff officials were unable to provide information on vulnerability assessments for the nine newly added assets from non-ATF components to the MEI. According to IMSS officials, their queries to components were not answered.

C. Progress Toward Mitigating Critical IT Asset Vulnerabilities

(1) Background on Critical IT Asset Vulnerabilities

As previously stated, the March 2002 Vulnerability Assessment identified 12 categories of vulnerabilities among the 20 IT systems comprising the Department's mission-essential inventory. Sources used to identify the 12 information technology vulnerabilities included vulnerability assessments submitted with the C&A packages, OIG system audits, penetration testing, and results from the Department's IV&V program.²⁴ Based on guidance from the GSA, the vulnerability assessments focused on common attack methods and publicly available cyber-attack methods. As

²⁴ Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques developed by hackers.

established in the CIP Plan, highly esoteric threats and attack methods are to be deferred to the long-range implementation of the CIP program.

Several of the vulnerabilities could potentially allow great harm to the Department's ability to perform its essential national security missions and maintain order. JMD prioritized the vulnerabilities according to the potential effect each was assessed to have on critical IT systems. Listed below are the 12 IT asset vulnerabilities, which are further discussed in Appendix 8:

- lack of auditing features, audit trails, or policies and procedures;
- improper or inadequate password protection, password aging, and construction;
- lack of encryption;
- software patches not installed for known vulnerabilities;
- lack of, limited, or untested contingency plans;
- lack of computer security incident response capability;
- lack of access controls;
- lack of configuration management;
- lack of intrusion detection;
- lack of or inadequate virus protection;
- exploitable network services enabled; and
- lack of warning banners.

(2) Processes Used by the IMSS to Monitor Mitigation of the Critical IT Asset Vulnerabilities

For the IMSS to track and manage components' efforts to close security performance gaps, components need to document and report security weaknesses and progress of mitigation actions. Accordingly, in August 2002, the IMSS notified each component to develop Plans of Actions and Milestones (POA&Ms) to ensure identified security weaknesses are corrected. All Department officials would use the POA&MS as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps.

Because the Department's POA&M was initially due to the Office of Management and Budget (OMB) by October 1, 2002, the IMSS requested the components to submit individual system and component summary POA&Ms to the IMSS by September 13, 2002. In developing the POA&Ms, components were requested to identify all security weaknesses; indicate how weaknesses were identified (for example, CFO audits, penetration testing, and self assessment); show corrective actions; estimate completion dates; and identify resources required to remediate the IT system weaknesses. Once the POA&Ms were received from components, IMSS staff would then begin entering the data into the SMART database system.

We were told by IMSS officials that they use the SMART database system to monitor the status of the 12 IT asset vulnerabilities. The SMART system is a set of user interface, database management, and business intelligence tools designed to assist the Department CIO and program managers, as well as the security administrators, in identifying, controlling, and monitoring the performance of a component IT security program and its IT systems. During FY 2003, the SMART system is gradually becoming available to security analysts, administrators, and managers in all Department components.

Data pertaining to remediating IT asset vulnerabilities is entered into the SMART system as it is received from the components. Data entered includes all vulnerabilities identified, corrective actions taken or planned, estimated completion dates, resources required to initiate corrective actions in terms of time and dollars, and status (whether the corrective actions are closed or open). Certain data entry fields such as estimated completion dates, resources required, and actions closed are locked once the data is entered.

For SBU computer systems, IMSS officials indicated they had been entering component IT asset vulnerability data into the SMART system since April 2001. An IMSS official indicated that the POA&Ms have been received and entered into the SMART system, but IMSS officials did not provide all of the documentation that was requested regarding this effort. Specifically, IMSS officials did not provide the POA&M from the FBI or SMART data for systems for which the IMSS is tracking risk mitigation activity. Additionally, beginning in January 2003 components were required to provide the IMSS with quarterly updates on risk mitigation activities. Data from these updates were also to be entered in the SMART system. IMSS staff indicated that quarterly updates were being received and entered into the SMART system, but again did not provide documentation that we requested regarding this effort.

For classified computer systems, IMSS staff indicated that a tracking system is being developed into which classified vulnerability data will be entered. The system was expected to be ready for use by July 30, 2003. Twenty nine percent (6 of 21) of the assets are classified systems. The IMSS was unable to explain how tracking currently occurs for classified systems but described the current process as "weak."

Absent the requested documentation for tracking SBU systems and the stated weakness in tracking classified systems, we could not verify that mitigation of vulnerabilities is being properly monitored.

(3) Significant Weaknesses in the IMSS Monitoring of Mitigation Activities for Critical IT Asset Vulnerabilities

We identified the following significant weaknesses regarding the IMSS's efforts to monitor mitigation actions for the 12 critical IT asset vulnerabilities.

(a) POA&Ms Were Not Properly Completed by Components

The August 29, 2002, notification requiring components to develop POA&Ms also contained detailed preparation instructions. As stated in the notification, each component was required to prepare individual system and component summary POA&Ms describing all known IT security weaknesses. At the system level, components were to indicate the source of each weakness, corrective actions, and estimated completion dates.²⁵ Component summaries were required to include a cross-system summary of weaknesses, steps components were taking to correct weaknesses, and completion dates. Components were also required to describe the performance measures that would be used to track progress in mitigating weaknesses.

We evaluated the POA&Ms submitted by the DEA, INS, and JMD, three of the four components with critical IT systems identified in the 2001 MEI. We did not evaluate the POA&Ms submitted by the FBI. We initially requested the FBI information in October 2002. The FBI, at that time, had not provided data to the IMSS because the FBI was undergoing an intensive C&A of a portion of its systems. We updated our audit information in May 2003. Information Management and Security Staff officials indicated that the FBI had provided the IMSS with POA&Ms. We requested the FBI's POA&Ms from the IMSS, but the information had not been provided as of the date of our draft report.

²⁵ IT security weaknesses were identified through audits, system security penetration tests, self-assessments, and vulnerability assessments.

In the 2002 "Summary of the OIG Fiscal Year 2002 Evaluation of the Department of Justice Information Security Program and Practices Pursuant to the Government Information Security Reform Act" report submitted to the OMB, OIG auditors concluded that the Department had not performed timely and effective oversight to ensure implementation of Department security policies. This weakness was evidenced by the components' failure to implement corrective actions in their systems' environment.

Of the POA&Ms we evaluated, none were properly completed or fully usable for tracking mitigation actions for critical IT system weaknesses. Our specific concerns are noted below.

- Of the 43 risk items identified in the vulnerability assessments for the DEA, INS, and JMD critical IT systems, only 20 risk items were addressed in the POA&M submissions. Consequently, mitigation actions for most of the vulnerabilities identified in the Department Vulnerability Assessment were not addressed by components. Although the POA&Ms are intended to reflect existing plans to correct IT weaknesses, it appears that there are no plans to correct 23 of the known weaknesses.
- None of the components identified the source of weaknesses reported in POA&Ms. Consequently, we were unable to determine whether all sources of IT security weaknesses were considered by components in developing the POA&Ms.
- None of the components described the performance measures that would be used to track progress in mitigating weaknesses as required in the August 29, 2002, notification.
- JMD's POA&M was structured as a self-assessment questionnaire that, in our judgment, did not appear to us to be usable for monitoring mitigation actions.
- The DEA's POA&M did not include planned corrective actions.

Weaknesses in the POA&Ms appear to result in part from some problems with the Vulnerability Assessment on which the POA&Ms are based. The Vulnerability Assessment does not clearly identify the specific critical IT asset vulnerabilities needing mitigation, and the document contains some internal inconsistencies that could cause problems in preparation of the POA&Ms.

(b) POA&Ms Did Not Adequately Identify Required Resources for Implementing Risk Mitigation Activities

Based on the results of Vulnerability Assessments and the subsequent mitigation and response plans, there is the possibility that additional resources may need to be identified, developed, or procured to ensure the protection of the Department's critical infrastructure.

JMD's initial effort to identify budgeted resources to improve IT security for mission-essential systems is documented in the March 2002 Vulnerability Assessment. Section 5 of the assessment contains the multi-year funding plan that projects the Department will spend approximately \$314.5 million in FYs 2002 through 2004 to improve IT security. The funding details are contained in the table on the following page. We noted multimillion-dollar discrepancies in the totals submitted for the FBI, which the IMSS staff acknowledged as a math error. We corrected the table to include the Trilogy amounts in the FBI totals.²⁶

²⁶ The Trilogy program is the FBI's 36-month program to upgrade the infrastructure technologies throughout the FBI. It consists of three components: 1) Network - which includes high-speed connections linking FBI offices; 2) Information Presentation - which is comprised of hardware and software within each office to link each employee at their desk to FBI systems; and 3) User Applications - which includes several user-specific software tools to enhance each agent's ability to organize, access, and analyze information.

**Multi-Year IT Security Funding Plan
(FYs 2002 through 2004)**

	FY 02	FY 03	FY 04
Justice Management Division			
Critical Infrastructure Protection	\$71,135	\$123,366	\$125,833
Program Contract Support			
Justice Data Centers	\$2,302,200	\$1,583,000	\$1,617,330
Justice Consolidated Network	\$196,260	\$200,000	\$202,635
Component Total by FY	\$2,569,595	\$1,906,366	\$1,945,798
Drug Enforcement Administration			
Information Security Initiative	\$2,879,000	\$6,683,000	\$6,843,000
El Paso Intelligence Center Information System	\$163,400	\$477,000	\$747,000
Mercury (See Note #1)	\$0	\$0	\$0
Merlin	\$385,700	\$648,499	\$1,512,634
Firebird	\$2,201,100	\$18,053,400	\$18,053,400
Model 204 Applications	\$809,400	\$2,180,000	\$2,230,000
Component Total by FY	\$6,438,600	\$28,041,899	\$29,386,034
Federal Bureau of Investigation			
Information Assurance Initiative	\$58,573,000	\$74,570,000	\$39,981,000
Trilogy	\$13,214,520	\$1,430,320	\$2,901,760
Mainframes and Applications	\$574,294	\$750,000	\$759,924
Criminal Justice Information System (CJIS) WAN	\$193,800	\$452,000	\$452,000
InfraGard (See Note #2)	\$0	\$0	\$0
Integrated Automated Fingerprint Identification System (IAFIS)	\$408,910	\$316,696	\$316,210
National Crime Information Center 2000 (NCIC 2000)	\$268,690	\$202,463	\$207,750
Intelligence Information System (IISNET) (No Data provided)			
Secure Automated Messaging Network (SAMNET)	\$329,500	\$436,000	\$341,000
FBI Wide Area Network (FBI NET)	\$290,000	\$290,000	\$290,000
Component Total by FY	\$73,852,714	\$78,447,479	\$45,249,644
Immigration and Naturalization Service			
Atlas Project	\$4,351,000	\$17,998,000	\$18,870,170
Central Index System (CIS)	\$259,500	\$75,000	\$45,000
Enforcement Case Tracking System (ENFORCE)	\$1,449,250	\$985,525	\$734,598
Automated Biometric Identification System (IDENT)	\$651,700	\$646,500	\$638,950
Wide Area Network (INSINC) (See Note #3)	\$0	\$0	\$0
Component Total by FY	\$6,711,450	\$19,705,025	\$20,288,718
Total by FY	\$89,572,359	\$128,100,769	\$96,870,194
Total all FYs	\$314,543,322		
Notes #1 - Funding for Mercury is included in the funding for Merlin and the Information Assurance Initiative. #2 - No funding information available. #3 - Funding for INSINC is included in the funding for the Atlas Project .			

Source: JMD's March 2002 Vulnerability Assessment as recalculated by the OIG

Although the multi-year funding plan was an initial attempt to identify resources budgeted to improve IT security for mission-essential systems, it did not specifically identify whether sufficient resources were budgeted to remediate the vulnerabilities identified in the March 2002 Vulnerability Assessment. The plan was not linked to the identified vulnerabilities and is not useful in identifying whether the funding amounts presented are adequate to remediate IT systemic vulnerabilities. Accordingly, in the August 29, 2002, notification requiring components to develop POA&Ms, the IMSS also requested that components identify the resources required to mitigate vulnerabilities.

Of the three component POA&Ms that we reviewed, none adequately identified resources required to mitigate vulnerabilities.

- In its summary POA&M, the INS identified \$9,350,703 in additional funding required to mitigate known IT system vulnerabilities. However, in each of its supporting system-level POA&Ms, the INS indicated that no additional resources would be required to mitigate vulnerabilities. This discrepancy was apparently undetected by the IMSS's review of the INS's POA&M.
- The POA&M submitted by JMD did not address budgeted resources required to mitigate vulnerabilities.
- The POA&M submitted by the DEA contained a column for recording resources required to mitigate vulnerabilities; however, most of the column was blank.

We discussed with the IMSS staff these problems with the POA&Ms and asked why their review of the documents did not identify the problems. We were told by the IMSS staff that their review of the POA&Ms consisted of identification of security and planning issues. An IMSS analyst determines whether the planning and funding is adequate to remediate the identified weakness. If it is not, then the IMSS analyst will work with the component's representative to develop adequate plans. Information Management and Security Staff indicated that the INS probably included the \$9.3 million funding requirement in its Exhibit 300 for a new system and not to mitigate weaknesses in an older system.²⁷

²⁷ An Exhibit 300 is a capital asset plan that must be prepared for major projects and is submitted to the Department and OMB.

(c) Process Used to Monitor Components' Progress in Mitigating IT Asset Vulnerabilities Was Ineffective

The IMSS was responsible for monitoring components' progress in mitigating IT asset vulnerabilities by performing quarterly comparison of Exhibit 300s to data stored in the SMART database. The intent of these comparisons is to determine whether actions to mitigate vulnerabilities have been funded and whether mitigating actions are ongoing.

We identified several shortcomings with this process. First, such a comparison may not be effective in that the Exhibit 300s do not provide a sufficient level of detail regarding resources budgeted to mitigate vulnerabilities associated with critical systems. The Exhibit 300s provide a narrative of corrective action but do not consistently associate costs of mitigating specific vulnerabilities. For example, the FBI's Exhibit 300 included an estimate of \$569,123 for security costs of the NCIC 2000 system. The FBI's narrative explains that it will cover an audit log server system, additional intrusion detection capability, and a separate Intrusion Detection System (IDS) management network segment that collects firewall and IDS system log files. The FBI's Exhibit 300 does not provide a separate costing for the audit log server system from the additional intrusion detection capability.

At the time of our audit, the Department had not had adequate time to complete vulnerability assessments, risk mitigation plans, or multi-year funding plans for most of the assets newly added to the MEI. While the Department has efforts underway in each of the areas identified above, effective oversight is necessary if the Department is to provide adequate protection of its critical assets.

Second, such a comparison is unnecessary since components are required to identify in the POA&Ms whether required resources were identified and funded. However, the POA&Ms do not appear to be useful for this purpose.

Third, the comparison process was not summarized or documented; consequently, the IMSS was unable to show how much progress components had made in mitigating critical IT system vulnerabilities. The POA&Ms require follow-up guidance from the IMSS to be effective as a risk mitigation monitoring tool.

D. Conclusions

Through the efforts of the IMSS, the Department has made some progress in establishing and managing a risk mitigation program. The IMSS has accomplished:

- completion of vulnerability assessments,
- development of risk mitigation plans (though none properly completed),
- development of the SMART database to track risk mitigation for SBU systems,
- completion of drafting a new CIP Plan, and
- revalidation of MEI after September 11, 2001.

Despite this progress, significant problems remain in the Department's management of the risk mitigation program. The major weaknesses that remain are identified below.

- Identification of critical assets from the ATF has yet to be completed.
- Vulnerability assessments, risk mitigation plans, and a multi-year funding plan were not developed for assets newly added to the MEI and for those to be identified from the ATF.
- The IMSS has not developed a system to track risk mitigation for classified systems.
- Resources required to mitigate vulnerabilities were not adequately identified.
- Plans of Actions and Milestones were not adequately completed by components.

The Department has not had adequate time to make a vulnerability assessment or risk mitigation plans for assets newly added to the MEI and for assets transferred from the ATF. While the Department has efforts underway in each of the areas identified above, effective oversight is necessary if the Department is to provide adequate protection of its critical assets.

Our audit work disclosed that the IMSS did not establish an effective Department risk mitigation program and that the IMSS's efforts to monitor mitigation actions were not effective. Regarding the four program vulnerabilities, IMSS officials indicated that mitigation actions were progressing on schedule. However, we initially found that the IMSS did not effectively manage the mitigation actions in that project plans were developed but lacked key milestone dates for completion, and the IMSS did not allow components sufficient time to provide required data.

Regarding the mitigation of the 12 critical IT asset vulnerabilities, we found that the POA&Ms, which were required to ensure the correction of identified security weaknesses, were inadequately prepared by components. None of the POA&Ms identified required resources for implementing risk mitigation activities. Additionally, the process used by the IMSS to monitor components' overall progress in mitigating vulnerabilities was ineffective.

These problems occurred, in part, because IMSS officials did not evaluate the effectiveness of their many risk mitigation-monitoring activities. Although IMSS officials were fully aware of the PDD 63 requirement for achieving full operating capability by May 2003, the Department has not met this requirement. In its revised CIP Plan, key activities are identified but some do not include milestone dates for completion. Further, although the IMSS required components to prepare and submit risk mitigation plans, a thorough review would have disclosed that the plans contained several deficiencies. Although the IMSS was expending considerable resources to enter data from the component risk mitigation plans into its SMART database system, the process used to assess components' progress in mitigating critical risks was ineffective. Also, no system was established for monitoring risk mitigation of classified systems.

As a result of these deficiencies, the Department has not achieved the mandated "full operating capability" and has less than adequate assurance that critical IT asset vulnerabilities will be adequately or timely mitigated.

E. Recommendations

We recommend that the Assistant Attorney General for Administration:

1. Develop a tracking system for risk mitigation activities for classified MEI systems.
2. Develop a multi-year funding plan based on resources required to mitigate vulnerabilities as identified in revised POA&Ms.

3. Revise the current process used to monitor components' progress in mitigating critical IT vulnerabilities to a clear component-by-component summary.
4. Monitor and document, at least quarterly, the status of certification and accreditation for critical IT systems.
5. Ensure components submit POA&Ms completed in accordance with OMB guidance. At a minimum, the component's POA&Ms should:
a) clearly address the vulnerabilities identified in the Department Vulnerability Assessment, b) include the source of the vulnerabilities so readers can refer back to the Department Vulnerability Assessment to obtain additional information, c) describe the performance measures used to track progress in mitigating weaknesses, and d) identify resources required for implementing risk mitigation activities for each identified vulnerability.
6. Conduct vulnerability assessments and develop risk mitigation plans for assets newly added to the MEI.
7. Determine the critical assets within the ATF and perform vulnerability assessments, develop risk mitigation plans, and a multi-year funding plan for those assets.
8. Develop a work plan, with milestone dates for key activities, for attaining full operational capability for critical infrastructure protection at the earliest possible date.

2. ESTABLISHING AN EMERGENCY MANAGEMENT PROGRAM

Although the April 1999 CIP Plan contained a comprehensive blueprint and milestones for an effective, centrally managed Department emergency management program, such a program has not been fully implemented. Many of the critical emergency management program elements relating to indications and warnings, incident collection, reporting and analysis, and response and contingency planning were neither established nor operating. Although the CIP Task Force was responsible for developing and implementing the CIP Plan, including the emergency management program, the Task Force ceased operating during calendar year 2000 and had no further involvement in implementation activities. As a result, the Department has less than adequate assurance that it can effectively respond to computer attacks and security incidents.

A. Department Efforts to Establish an Emergency Management Program for the Protection of Critical Infrastructure Assets

The April 1999 CIP Plan established the critical elements for an effective emergency management program and tasked the CIP Task Force (CIPTF) with its implementation. The CIPTF had members in 9 law enforcement entities, 5 litigating divisions, and 12 other entities. See Appendix 10 for Department entities that had CIPTF members. The Department's emergency management program, as envisioned in the CIP Plan, was to incorporate the following three elements.

- **Indications and Warnings:** The purpose of this element was to establish an effective and secure mechanism for: a) receiving threat indication and warning information concerning the critical infrastructure of the Department and the nation from the intelligence community and law enforcement agencies, and b) disseminating this information in a timely manner to appropriate Department components.

As envisioned in the CIP Plan, the emergency management program would establish effective liaisons with the Department's SEPS, the FBI's NIPC, and the FBI's Strategic Information Operations Center (SIOC). The IMSS would ensure the existence of secure, effective, and timely communication channels for passing threat information from internal and external organizations to Department components at

both headquarters and field locations charged with the protection of the Department's critical infrastructure assets.²⁸ In our judgment, although part of the NIPC has been transferred to the DHS, an effective liaison capacity is still needed.

- **Incident Collection, Reporting, and Analysis:** This element was to define and establish an effective and secure mechanism for collecting, reporting, and analyzing incident information about actual and potential attacks on the Department's critical infrastructure assets.²⁹ The established method should have ensured that information generated from computer security incidents was received from Department components and disseminated throughout the Department and to other intelligence and law enforcement agencies, as appropriate, in a timely manner.

Incident data would be provided to the NIPC as part of the National Critical Infrastructure Indications and Warnings System and the Department's Computer Security Laboratory to establish new requirements for a research and development program. The incident data would also be used to support budget and resource justifications.

- **Response and Contingency Plans:** This element was to define and establish sound response and contingency plans to ensure that the Department's critical infrastructure assets could be restored to the minimum operational effectiveness necessary to support the Department's missions, should these critical infrastructure assets be subjected to successful attack.

Response plans identify actions for responding to a significant infrastructure attack while the attack is underway. Contingency plans identify actions required to rebuild or restore an infrastructure after it has been damaged. The CIP Plan requires that response and contingency plans should be prepared, reviewed, and approved by Department authorities, and tested by an exercise on a periodic basis to ensure that the plans can be effectively implemented.

The CIP Plan also established several intermediate milestones for implementing the three essential elements of the Department emergency

²⁸ The CIP Plan did not contain details as to how the communication channels would operate or how the communication channels would be implemented.

²⁹ An incident is an occurrence that has been assessed as having an adverse effect on the security or performance of an information system.

management program. Full implementation of the program was to occur no later than September 28, 1999.

B. Implementation of the Emergency Management Program

Although the CIP Plan contained a comprehensive blueprint and milestones for an effective, centrally managed Department emergency management program, such a program was never fully established. Officials of the IMSS indicated that the CIP Task Force, tasked with implementing the emergency management program, last met during calendar year 2000 and was no longer in existence. In response to our inquiries, those IMSS officials could not provide an explanation as to why no further effort was made to implement the plan.

Officials of the IMSS also stated that although the emergency management program as envisioned in the CIP Plan had not been implemented, most of the elements of an effective emergency management program were nevertheless in place and operating throughout the various Department components. However, in evaluating the Department's response capabilities to computer security incidents, we found that many of the four critical emergency management program elements relating to 1) indications and warnings, 2) incident collection, reporting and analysis, 3) response plans and 4) contingency planning were neither established nor operating. Our specific observations follow.

(1) Indications and Warnings

The IMSS did not ensure that this element of the emergency management program was fully implemented. According to JMD officials, communication channels were established for passing threat information from internal and external organizations to Department components at both headquarters and field locations charged with protecting the Department's critical infrastructure assets. Specifically, the DOJCERT is the Department's central point for receiving and disseminating indications and warnings.³⁰ Within the DOJCERT, a contractor operates the Department's-Information Sharing and Analysis Center and provides a departmentwide mechanism for sharing vulnerabilities to better prepare the Department for responding to cyber attacks. Additionally, the DOJCERT has implemented an intranet web

³⁰ In May 2003, the IMSS name changed to the Information Technology Security Staff (ITSS). The ITSS retained the prior IMSS staff and responsibilities for oversight of the CIP program. The ITSS gained responsibility from JMD Computer Services Staff for managing the DOJCERT.

page that includes a search capability for previously distributed indication and warning bulletins, and an Internet web page for information purposes.

Although communication channels were established for passing threat information, the IMSS did not determine whether the channels were secure, effective, and provided timely information as required by the CIP Plan. Additionally, the IMSS did not verify whether effective liaisons with the FBI's NIPC or the SIOC were established and ongoing. See Finding 3 for more details concerning liaisons not being adequately identified. Unless all indication and warning elements are in place, the Department does not have the assurance that communication channels for sharing vulnerabilities are secure and that components are receiving timely information to better equip them to respond to computer security incidents.

(2) Incident Collection, Reporting, and Analysis

The IMSS did not ensure that this element of the emergency management program was fully implemented. Although detailed procedures for components to follow when reporting computer security incidents were developed, the IMSS did not verify that these procedures were implemented and being followed, nor did the IMSS ensure that security incident data was being collected and analyzed.

The JMD CSS developed the June 27, 2002, Standards, Guidelines, and Standard Operating Procedures for the DOJCERT (Department Manual TP-001). This directive was developed in response to an increase in computer attacks and contains detailed procedures for effective handling and reporting of computer security incidents. Department Manual TP-001 identifies and defines the following nine computer security incident categories.

- **System Compromise:** An unauthorized user gains system privileges on Department computers.
- **Information Compromise:** A weakness in a Department system is exploited that allows unauthorized access to password files, protected or restricted data, system resources, and software/code but does not gain system privileges.
- **Unauthorized Access:** A valid Department account is used without permission of the owner.
- **Denial of Service:** Department resources are unavailable for use by an authorized user.

- **Misuse:** An authorized user violates federal law or regulations and/or Department policies regarding proper use of computer resources, installs unauthorized or unlicensed software, or accesses resources or privileges that are greater than those assigned.
- **Hostile Probes:** One or more systems are used to scan targeted Department systems or networks with the intent to conduct or to gather information for unauthorized or illegal activities.
- **Malicious Software:** Software developed with the intent to run on and cause harm to Department computers.
- **Intrusions:** Access by unauthorized individuals to Department systems that bypasses authentication mechanisms, exploits vulnerabilities in system services, eavesdrops, or monitors networks.
- **Theft:** Unauthorized removal of Department information and computer equipment.

Because incidents may have many possible consequences ranging from slight to catastrophic, Department Manual TP-001 outlines five priorities to consider when evaluating and dealing with computer security incidents.

- **Priority 1:** Protect human life and people's safety.
- **Priority 2:** Protect National Security Information (NSI) data.
- **Priority 3:** Protect SBU data.
- **Priority 4:** Prevent system damage.
- **Priority 5:** Minimize disruption of computing resources.

The Department Manual TP-001 also contains detailed reporting requirements for components to follow in reporting computer security incidents. For incidents involving SBU systems, components are required to provide the DOJCERT a verbal report within one working day after an incident has occurred. Within five working days, a written preliminary incident report, containing as much information as possible, is to be submitted. Within ten working days of the resolution of an incident, a written formal report is to be submitted, and in cases where incident resolution is expected to take more than 30 days, a status report is to be

submitted to the DOJCERT every 10 days. For incidents involving NSI, components follow the same reporting requirements with the exception that the reports are provided to the Department Security Officer rather than to the DOJCERT.

Although detailed procedures were developed by the CSS for components to follow in reporting computer security incidents, the IMSS could not substantiate whether the procedures were implemented and were being followed. According to IMSS staff, tabulated summaries on the number and type of incidents are reported each month. However, the IMSS could not provide tabulated summaries regarding the nature, frequency, category, and remediation of prior Department computer security incidents or possible trends and potential systemic weaknesses based on analyses of prior incidents. In addition, the IMSS did not verify whether additional procedures for collecting and analyzing incidents as required by the CIP Plan were developed and in place. We asked the IMSS for an explanation why no verification of additional procedures occurred but the IMSS officials provided no response. Although there is no specific requirement that the IMSS maintain documentation for these activities, absent such documentation, the Department does not have the assurance that additional procedures for collecting and analyzing incidents as required by the CIP Plan were developed and in place.

Absent the documentation described above, the IMSS will have little assurance that it is developing effective countermeasures from prior attacks and providing this knowledge to components to enhance response capabilities.

(3) Response Plans

We determined that the IMSS did not fully implement this element of the emergency management program. Although requirements had been established for developing, implementing, and testing incident response procedures, the IMSS did not verify whether the procedures were in place and operating.

Department Manual TP-001 requires each Department component to: a) develop, implement, and maintain internal incident response procedures, and b) identify an appropriate individual responsible for reporting incidents to the DOJCERT. The Manual also provides the minimum level of procedures for component incident response programs and specifies that the response procedures should be documented by each component and submitted to the DOJCERT to be kept on file.

In addition to developing Department Manual TP-001, JMD CSS also developed the June 17, 2002, DOJCERT Procedures Manual, which outlines CSS Service Center and DOJCERT procedures for responding to Department computer security incidents.³¹ In responding to an incident, the CSS Service Center assigns a number to the incident and completes an incident report form that is forwarded to an incident manager then to the DOJCERT program manager for investigation and resolution.³²

Upon notification of the incident, the DOJCERT Program Manager performs an initial assessment by: a) reviewing the incident report to determine the severity of the problem; b) locating sources and organizing steps for solutions; c) determining who should be notified and involved in working the solution; d) determining whether a Security Alert needs to be broadcast;³³ and e) determining whether the FBI, NIPC, Federal Computer Incident Response Center (FedCIRC) or SEPS need to be notified.³⁴ After completing the initial assessment, the Program Manager then initiates the solution identified during the assessment process and updates the ticket management system with information about the implemented solution and the incident response process.

Although detailed response procedures for computer security incidents had been established, the IMSS had not ensured that the procedures were implemented and being followed. Specifically, the IMSS did not verify whether components had developed, implemented, and maintained internal incident response procedures and whether components had identified appropriate individuals responsible for reporting incidents to the DOJCERT. Although there is no specific requirement that the IMSS maintain documentation for these activities, absent such documentation the Department does not have assurance that response procedures are effective.

³¹ The CSS Service Center was the front-end support for the DOJCERT incident and inquiry response operations. In most cases, the Service Center was the initial point-of-contact or first-level support for the DOJCERT operations staff. Since May 4, 2003, the incident and inquiry response functions have moved to the ITSS.

³² The Program Manager is responsible for directing and managing the personnel and operations of the DOJCERT.

³³ A Security Alert should be sent under the threat and warning reporting procedures if the incident has affected or is likely to affect more than one component.

³⁴ Within the DHS, the FedCIRC is the central coordination and analysis facility dealing with computer security-related issues affecting the civilian agencies and departments of the federal government.

In May 2003, we sought any changes in these procedures. Information and Management Security Staff indicated that they were able to provide summary information on computer incidents, but as of June 6, 2003, no documentation had been provided.

In a 2002 review of the FBI's Automated Case Support System pursuant to the GISRA, OIG auditors determined that the FBI is not following the incident response requirements outlined in Department Manual TP-001.³⁵ Specifically, personnel had not been formally trained to identify and handle incidents and the incident response procedures had not been centralized or implemented across the FBI. This condition occurred because the FBI had not yet developed incident response procedures that meet the requirements of the DOJCERT or trained employees in the incident response procedures and requirements. As a result, the FBI increased its risk of having incidents occur without its knowledge or proper follow-up. Had the IMSS verified implementation of the DOJCERT requirement, such lapses in complying with incident response requirements could have been avoided.

Additionally, although the CIP Plan requires periodic testing of response plans, such testing had not been conducted. Information Management and Security Staff officials maintained that response plans were in fact tested during the last major incident involving a computer worm; however, a response during a single actual incident does not constitute complete testing of the response plans because some aspects of the plan may not be involved in the response to a single live incident.³⁶ The IMSS officials added that testing was also unnecessary because they frequently received component warnings from the DOJCERT. They reasoned they could only receive such warnings if the response plans were working. We disagree with this reasoning because a single incident may test some aspects of a response plan while a complete test would check all aspects of the response plans. Testing of response plans is crucial to identifying weaknesses prior to the occurrence of an actual incident.

³⁵ See "Independent Evaluation Pursuant to the Government Information Security Reform Act Fiscal Year 2002" (Audit Report 03-06).

³⁶ A computer worm is a program that replicates itself and often contains some functionality that interferes with the normal use of a computer or program. Unlike viruses, worms exist as separate entities spreading automatically over networks from one computer to the next.

(4) Contingency Plans

We determined that the IMSS did not fully implement this element of the emergency management program. Although requirements had been established requiring components to develop and periodically test contingency plans, we found that the majority had not done so.

On July 12, 2001, the JMD Information Management and Security Office issued the Department Order 2640.2D, requiring components to develop contingency plans for: a) continuing missions in the event IT systems become unavailable, and b) recovering IT systems in event of loss or failure. In complying with the Department Order, components must ensure that contingency plans:

- identify the priorities of the system for restoration, taking into consideration the system's role in fulfilling the Department mission and interdependency requirements;
- determine the maximum amount of elapsed time permissible between an adverse event and putting the system's contingency plan into operation;
- determine the maximum amount of data and system settings that can be lost between the service interruption event and the last back-up (this measure determines system back-up policies); and
- identify interdependencies with other Department of Justice, state, or local agency systems that could affect contingency operations.

The Department Order also requires components to: a) test contingency resumption plans annually or as soon as possible after a significant change to the environment that would alter the in-place assessed risk, and b) develop and maintain site plans detailing responses to emergencies for IT facilities.

Although the Department Order required components to develop and test contingency plans as well as site plans detailing responses to emergencies for IT facilities, the IMSS could not provide support that components had done so. We noted the following deficiencies.

- From the January 2001 MEI, the IMSS was able to provide contingency plans for 12 of the 20 critical IT systems. In regard to the other eight systems, IMSS officials explained that: a) for six of the classified systems, the contingency plans were kept with SEPS, b) the

contingency plan for one system was being updated, and c) for two systems the plans were no longer relevant since the systems were being reengineered and were not operational.³⁷ Although these explanations as to why the IMSS did not have contingency plans were plausible, the explanations were not supported by any documentation. Absent such documentation, it is not evident that the IMSS was carrying out its assigned oversight responsibilities.

We updated the audit information in key CIP areas in May 2003. From the December 2002 MEI, the IMSS was able to provide contingency plans for only 9 of the 21 critical IT systems. According to IMSS officials, the classified files had been transferred from SEPS to the IMSS. Information Management and Security Staff officials explained that the DEA housed their own contingency plans at various locations. When asked to provide documentation of the IMSS's review of the DEA contingency plans, IMSS officials were not able to provide any. Information Management and Security Staff stated that SEPS maintained very few contingency plans for the FBI. As a result, few FBI files were transferred to the IMSS. We attempted to review the FBI contingency plan but were not provided those plans by IMSS. Additionally, IMSS staff indicated that they were in the process of putting the FBI on a performance plan for the development of contingency plans for its systems without plans.

- Contingency Plans did not contain all elements required by Department Order 2640.2D. We judgmentally selected and reviewed contingency plans for the INS's INSINC System and the Department's CJIS WAN. As demonstrated in the following table, our review disclosed that required elements were not addressed for either contingency plan. This condition occurred, in part, because neither contingency plan showed coordination or approval actions by either the component or IMSS officials.

³⁷ The DEA's EIS consists of a classified and unclassified portion. IMSS possessed a copy of the contingency plan for the unclassified portion but not for the classified portion. This difference results in EIS being counted twice even though there are only 20 systems that comprise the January 2001 MEI. See Appendix 5 for more detail.

Evaluation of INSINC and CJIS WAN Contingency Plans

Required Element	INSINC	CJIS WAN
Identify system priorities for restoration.	Not Addressed	Not Addressed
Determine maximum amount of elapsed time permissible between an adverse event and putting the contingency plan in operation.	Not Addressed	Not Addressed
Determine the maximum amount of data and system settings that can be lost between the service interruption event and the last back-up.	Not Addressed	Not Addressed
Identify interdependencies with other systems.	Addressed	Not Addressed
Identify system owners, roles, and responsibilities.	Addressed	Addressed

Source: OIG analysis

In the 2002 "Summary of the OIG Fiscal Year 2002 Evaluation of the Department of Justice Information Security Program and Practices Pursuant to the Government Information Security Reform Act" report submitted to the OMB, OIG auditors found that the Department had weaknesses in contingency planning. This weakness was identified as a repeat weakness from the 2001 OIG report.

- Contingency plans were not tested annually as required by Department Order 2640.2D. As discussed previously, the Department first established its MEI of 20 computer assets in January 2001. This inventory was revised in December 2002 and the resulting MEI consists of 21 computer assets. Only three of the systems included on the January 2001 MEI had undergone contingency plan testing. One system with a tested contingency plan was dropped from the December 2002 MEI and another with a tested contingency plan was added. IMSS officials could not determine the status of contingency plans testing for any of the remaining eight assets newly added to the MEI as of May 2003. None of the other systems that remained from the January 2001 MEI had tested contingency plans. IMSS officials were unable to determine the status of the newly added assets because they received no response from the components to their queries. IMSS officials explained that testing of contingency plans was expensive and funds were not available; however, they were unable to provide documents showing that funding had been requested and denied. IMSS officials indicated that the Department's Chief Information Officer had intended to issue a memorandum to components stressing the importance of testing contingency plans and

providing guidance on how to perform and obtain funding to pay for the tests. As of May 2003, the document had not yet been issued.

C. Overall Causes for and Effect of Not Fully Implementing an Emergency Management Plan

Although the CIP Task Force was charged with developing and implementing the Emergency Management program, the Task Force never did so. Information Management and Security Staff officials stated that the Task Force last met during calendar year 2000 and was no longer in existence. They added that the Task Force's primary responsibility when it did meet was to work on Year 2000 conformity issues.³⁸ According to an IMSS official, once the Year 2000 conformity issues were resolved, the task force no longer convened. In response to our inquiries, IMSS officials could provide no explanation as to why no further effort was made to implement the plan.

Further, the IMSS officials stated that although the emergency management program as envisioned in the CIP Plan had not been implemented, they believed that most of the elements of an effective emergency management program were nevertheless in place and operating throughout the various Department components. We do not agree with this assessment because several of these elements are not adequately operating. Unless a centralized effort is made to verify that the various component parts of the CIP Plan are in place and operating, the Department will have little assurance that it can effectively respond to emergency computer security incidents.

D. Conclusions

Although the CIP Plan contained a comprehensive blueprint and milestones for creating an effective emergency management program by September 1999, such a program was not fully implemented as demonstrated in the following table.

³⁸ Year 2000 conformity ensured that Departmental IT system performance and functionality would not be affected by dates prior to, during, and after the year 2000.

Implementation of the Department's Emergency Management Program to Protect Critical Infrastructure IT Systems

CIP Plan Requirement	Element Implemented	Element not Implemented
Indications and Warnings	<ul style="list-style-type: none"> • Communication channels established for passing threat information 	<ul style="list-style-type: none"> • No verification to determine whether communication channels were secure, effective, and timely • No verification to determine whether required liaisons were established
Incident Collection, Reporting, and Analysis	<ul style="list-style-type: none"> • Requirements established for components to report incidents 	<ul style="list-style-type: none"> • No verification to ensure established procedures were followed by components • No verification to ensure incident data was being collected and analyzed
Response Plans	<ul style="list-style-type: none"> • Requirements established for developing, implementing, and testing incident response procedures 	<ul style="list-style-type: none"> • No verification to ensure response procedures were implemented and followed • Response plans not tested
Contingency Plans	<ul style="list-style-type: none"> • Requirements established calling for components to develop and test contingency plans 	<ul style="list-style-type: none"> • No support that plans were developed for all critical systems • Plans did not address all required elements • Plans not tested

Source: CIP Plan and OIG analysis

In evaluating the Department's response capabilities to computer security incidents, we found that many critical elements related to indications and warnings, incident collection, reporting and analysis, and response and contingency planning were neither established nor operating. We agree that other elements are operating, but not adequately for a successful emergency management program. Until the critical elements of an effective emergency management program are in place and operating,

the Department will have less than adequate assurance that it can effectively respond to attacks to its critical infrastructure technology systems.

E. Recommendations

We recommend that the Assistant Attorney General for Administration:

9. Define standards for secure, timely, and effective communication channels for passing indications and warning information and ensure those standards are implemented and operating.
10. Ensure that effective liaisons are established with the DHS's FedCIRC and the FBI's Strategic Information Operations Center and NIPC.
11. Ensure that components are in compliance with procedures for reporting incidents.
12. Ensure that data regarding departmentwide computer attacks and security incidents are collected and summarized according to the nature, frequency, category, and remediation actions taken and that analyses are performed to identify potential trends and systemic weaknesses.
13. Verify that incident data is provided to: a) the NIPC as part of the National Critical Infrastructure Indications and Warnings System, and b) the budget processes to support and justify future CIP resource expenditures.
14. Verify that components have developed, implemented, and maintained internal incident response procedures and have identified appropriate individuals for reporting incidents to the DOJCERT.
15. Ensure periodic testing of response plans.
16. Develop contingency plans for all critical IT assets.
17. Ensure that documentation is maintained supporting the existence or development of contingency plans for all critical infrastructure assets.
18. Verify that contingency plans address all required elements as identified by Department Order 2640.2D.

19. Obtain appropriate approvals for all contingency plans by component and IMSS officials.
20. Test contingency plans periodically as required by Department Order 2640.2D.

3. ESTABLISHING AN EFFECTIVE INTERAGENCY COORDINATION PROGRAM

The Department has not implemented an interagency coordination program, as required by the CIP plan. The Department's CIP Plan requires Department components to develop a list of liaison and interagency relationships for the CIP Task Force to develop and maintain a database of those relationships. The CIP Task Force, tasked with the development and maintenance of the interagency coordination database, was disbanded in 2000 without developing the database or addressing any of the CIP elements. Additionally, the Department has not determined the support its assets provide to other federal agencies and entities. This was caused in part because the IMSS did not require complete information from Department components in determining the Department's MEI. Without taking these steps, the Department cannot ensure effective coordination links exist and that information will be accessible from Department assets when needed.

A. Importance of Establishing an Effective Interagency Coordination Program

There are two primary objectives for establishing effective interagency coordination relating to CIP. First, the CIP Plan requires the Department to establish and maintain effective liaisons with entities proposing and promulgating security measures and plans relating to CIP. Doing so ensures that the Department receives and is aware of the most up-to-date information for protecting its critical IT asset systems.

Second, the CIAO's "Practices for Securing Critical Information Assets" provides guidance for the Department to identify and characterize the level to which Department assets provide support to other government agencies. As part of that process, the Department should establish and maintain effective liaisons with all entities for which Department IT systems either receive or provide critical data supporting national security, national economic security, and crucial public health and safety activities. All Department IT systems either receiving or providing such information must be identified and included in the Department's MEI as critical IT assets and receive the special protection afforded under the CIP program.

Establishing and maintaining effective interagency coordination in protecting the Department's critical IT asset systems is essential. The Assistant Attorney General for Administration, in approving the April 1999

Department's CIP Plan, recognized the importance of interagency coordination by stating in the plan that, "In general, we believe the quickest and most effective way to achieve a much higher level of protection from the threats to our critical infrastructure is through the sector structures in partnership with the owners, operators and appropriate government agencies."

B. CIP Plan Requirements for Establishing an Effective Interagency Coordination Program

The April 1999 CIP Plan addressed the need for cooperation with the various federal, state, and local agencies involved in the protection of the critical infrastructure as it pertained to Department operations. The CIP Plan addressed this need by defining and establishing the specific liaisons necessary for the Department to implement a sound CIP program. Liaisons were to be established at the national level between program elements located at Headquarters and their appropriate counterparts, as well as at the state and local levels for Department field offices. The CIP Plan established the following requirements.

- Each headquarters Program office was to identify current federal and interagency liaisons associated with CIP.
- Field offices were to identify to each Headquarters Program office all new and existing liaisons and memoranda of understanding with federal, state and local entities when these liaisons relate to CIP.
- The Department was to establish a method for ensuring coordination between the various Department entities and liaisons with outside organizations as these liaisons relate to CIP.
- The identification of these relationships was to be forwarded to the CIP Task Force. Each relationship forwarded to the Task Force was to include the organizations involved, Department representative(s), reason for the liaison, Department obligations, special considerations, and the primary mission of the outside organization.
- The CIP Task Force was to maintain the overall database of the liaisons and relationships, and serve as the Department's focal point for all liaisons and relationships pertaining to CIP.
- By May 7, 1999, the Department was to establish a working group or other means of communication in order to ensure that information was effectively shared between Department components having interagency relationships and liaisons.

C. An Interagency Coordination Program as Envisioned in the CIP Plan Was Not Implemented

Although the CIP Plan contained comprehensive requirements for implementing an effective interagency coordination program, as detailed below, such a program was never established within the Department.

- IMSS officials did not ensure that components' headquarters and field offices developed lists of current federal and interagency liaisons and memoranda of understanding associated with CIP.
- The Department had not established a method for ensuring coordination between the various Department entities and liaisons with outside organizations, as these liaisons relate to critical infrastructure protection.
- Components had not forwarded to the IMSS lists of liaisons and relationships. Consequently, the centralized database of liaisons and relationships was not created and maintained, nor is any entity within the Department serving as the focal point for all liaisons and relationships pertaining to CIP.
- A working group, or other means of communication, was not established to ensure that information is effectively shared between Department components having interagency relationships and liaisons.

D. Reasons Why an Effective Interagency Coordination Program Was Never Established

A primary reason for the lack of an interagency coordination program is that the CIP Task Force charged with serving as the focal point and maintaining the needed database did not address any of the CIP elements related to interagency coordination. The Task Force last met during calendar year 2000 and no longer exists. There were two reasons why the interagency coordination program as envisioned by the CIP Plan had not been implemented.

First, IMSS officials maintained that in developing the Department's MEI for IT assets, no Department IT system either received critical data from external entities or provided data to external entities supporting national security, national economic security, and crucial public health and safety activities. Second, IMSS officials maintained that ongoing activities within Department components effectively monitored interagency activity. For

these reasons, IMSS officials believe that there was no need to implement a vigorous interagency coordination program as called for in the CIP Plan.

However, we concluded that: a) the IMSS did not properly determine whether critical exchanges of information were ongoing between Department components and other entities, and b) ongoing activities within Department components did not adequately compensate for the lack of an effective interagency coordination program as required by the CIP Plan.

(1) IMSS Did Not Properly Determine Whether Critical Exchanges of Information Were Ongoing Between Department Components and Other Entities

In identifying critical IT systems, guidance published by the CIAO states that federal agencies were initially required to develop an inventory of all candidate IT systems. To identify the critical IT systems from the list of candidates, agencies could complete an Infrastructure Asset Evaluation Survey. This survey, developed by the CIAO, identifies seven “goals” and specific functions within each goal that are characteristic of goals and functions performed by critical IT systems. The goals identified in the survey were:

- perform essential national security missions,
- support state and local governments’ ability to maintain order,
- ensure orderly functions of the economy,
- ensure the general public health and safety,
- deliver minimum essential public services,
- determine the dependency of other government programs on the Department’s IT systems (involving critical exchanges of information), and
- ensure delivery of essential private sector services.

Although there is no hard and fast rule for determining what is or is not a critical IT system, in general the more goals an IT system supports – and the more significant functions the system performs within each goal – the more important the IT system is. The more important the IT system is, the higher the chances that the system will be identified as a critical asset.

We determined that the IMSS did not follow CIAO guidance in identifying its critical IT assets. IMSS officials did not require components to develop initial inventories of critical IT assets based on the Infrastructure Asset Evaluation Surveys of all candidate systems. Instead, components were requested early in calendar year 2000 to develop their inventories based on a four-tiered Impact Level Rating Scheme as described in the following chart.

Impact Level Rating Scheme

Impact Level	Description
1	<p><i>Would the loss of the asset:</i></p> <p>Prevent the Department from fulfilling its mission, critical national security or national security functions, or from providing continuity of core government services. <i>(Systems that fall in this category constitute critical assets.)</i></p>
2	Significantly debilitate the ability of the Department from fulfilling its mission, critical national security or national security functions, or from providing continuity of core government services.
3	Somewhat interfere with the Department's ability to fulfill its mission, critical national security or national security functions, or from providing continuity of core government services.
4	Have no appreciable impact on agency missions.

Source: IMSS Instructions for Selecting Critical Assets

This approach provided little assurance that candidate IT systems were adequately evaluated against the more comprehensive seven goals and the corresponding functions within each goal identified in the Infrastructure Asset Evaluation Survey. For example, unlike the Infrastructure Asset Evaluation Survey, the Impact Level Rating Scheme did not require components to consider dependency of other government programs on the Department's IT systems and whether critical information exchanges were occurring.

It was only after components had already developed their initial inventories of critical IT assets that the IMSS provided components with the Infrastructure Asset Evaluation Surveys. For each critical IT system identified, components were instructed to complete the survey for only one of the seven goals identified in the survey. The survey goal selected for

completion was to be determined by the primary goal actually supported by each critical IT system.

We identified two significant deficiencies with this approach. First, the purpose of the surveys was to identify critical IT systems from a list of candidate systems. Using the surveys on an already existing list of critical IT systems selected under a less comprehensive methodology was of questionable benefit. Second, IT systems may possess several goals characteristic of a critical IT system. Requiring components to complete a survey for only one of the seven goals risks overlooking other goals that may, upon closer analysis, elevate IT systems to critical status.

The net effect of these weaknesses in identifying the Department's critical IT systems is that neither the IMSS nor the Department components considered the dependency of other government programs on the Department's IT systems, and whether critical exchanges of information were occurring. As a result, Department IT systems that exchanged critical information may not have been identified and considered for protection under the CIP program.

Evidence that such exchanges of critical information may be occurring was documented in a November 13, 2001, memorandum to Department CIOs. In that memorandum, the Acting Assistant Attorney General for Administration stated:

The recent attacks of September 11, 2001, on the United States underscore the critical need for the Department of Justice to take an aggressive role in preventing aliens who engage in or support terrorist activity from entering the United States . . .

Information technology is a tool that can be used to fight terrorism through improved information sharing with other federal agencies. Through information sharing the overall investigative and intelligence analysis capabilities of the federal government can be enhanced . . . Towards this end, I have initiated an effort within JMD to summarize the current information exchanges between the Department, the Department of State, and the United States Customs Service.

A draft diagram and a description of the information flows as currently understood by JMD have been prepared. This diagram and the associated narrative provide an overview of the structured information exchanges between four Department

components, the Department of State, and the United States Customs Service.

The diagram provided by the Acting Assistant Attorney General is presented in Appendix 9. Although the draft diagram showed 19 FBI, DEA, and INS IT systems involved in information exchanges with the Department of State and the United States Customs Service, only 4 of these IT systems were identified by the Department as being critical in the January 2001 inventory and 2 were identified as being critical in the December 2002 inventory.³⁹ Information Management and Security Staff officials indicated that the Department received no critical information from external entities and indicated that if Department information is critical to the mission of the external entities, then the external entity representative should contact a Department representative. We previously noted in this report that liaisons had not been identified to facilitate the communication needed in this regard.

Among the remaining 17 systems not identified in either Department inventory are the FBI's National Instant Criminal Background Check System (NICS) and Automated Case Support (ACS) System, and the DEA's Narcotics and Dangerous Drugs Information System (NADDIS) as described below. We are not concluding that these are critical systems, but we believe that these systems provide important information to external entities. Without an assessment made in concert with external entities, the Department cannot ensure that its assets critical to the mission of other agencies have been adequately identified.

- **NICS:** The NICS allows firearms dealers to run background checks to ensure firearms are not sold to individuals who are prohibited from possessing firearms. The Department of State sends paper documents to the FBI identifying individuals who have renounced their United States citizenship. These individuals are listed in NICS as ineligible for firearm transfers.
- **ACS:** The Department of State transmits name check requests to the FBI over a secure network using magnetic tape. The names are checked against the FBI's ACS System. Paper notifications are sent back to the Department of State.
- **NADDIS:** The NADDIS system provides information to DEA personnel on people, businesses, vessels, and selected airfields identified through the

³⁹ The four IT systems identified as critical included the FBI's NCIC 2000 Database, the FBI's IAFIS, the INS's IDENT System, and the INS's CIS.

DEA investigative reporting system. The DEA provides a tape from NADDIS identifying persons to the Department of State on a monthly basis. The Department of State loads the identification into their Consular Lookout and Support System.

(2) Ongoing Activities Within Department Components Did Not Adequately Compensate for the Lack of an Effective Interagency Coordination Program.

The Department participates in two groups that have the potential to compensate for the lack of an effective interagency coordination program. These groups are the Information Technology Security Officers Working Group (ITSOWG) and the Computer Crime and Intellectual Property Section (CCIPS).

The ITSOWG is composed of the designated computer security officers or representatives from each of the components and JMD for the purposes of:

- providing a Department forum for discussing IT security issues, problems, and problem resolution;
- providing for the review and discussion of technological developments in the field of computer security;
- increasing components' awareness of IT security issues including threats to their environments;
- identifying security-related areas where Department standards and guidelines are lacking;
- assisting in the development of these standards and guidelines; and
- participating in the identification of IT security training needs.

A JMD official also meets periodically with a working group managed by the CCIPS of the Department's Criminal Division to establish uniform policy within the Department on computer crime issues. The CCIPS group advises federal prosecutors and law enforcement agents, comments upon and proposes legislation, coordinates international efforts to combat computer crime, litigates cases, and trains law enforcement groups.

Neither the ITSOWG nor the CCIPS group specifically addresses CIP issues. Absent a working group or other means of communication, the

Department cannot ensure that information between components is effectively shared and CIP issues are addressed.

According to IMSS staff, the IMSS partially identified the IT support provided by other agencies and its support to other agencies by developing a detailed analysis of systems and interrelations including the direction of the data flow. However, the IMSS's analysis does not provide all the data elements required by the CIP Plan, including organizations involved, Department representative, reason for liaison, Department obligations, special considerations, and the primary mission of the outside organization.

E. Conclusions

The Department's CIP Plan addressed the critical need for cooperation with the various agencies involved in the protection of the critical infrastructure. The CIP Plan defined and established the specific liaisons necessary for the Department to implement a sound CIP program. However, an effective interagency coordination program was not established because the Department did not: 1) ensure that components developed lists of current liaisons and memoranda of understanding associated with CIP; 2) establish a method for ensuring coordination between the various Department entities and liaisons with outside organizations; 3) create and maintain a centralized database of liaisons and relationships, or establish an entity within the Department to serve as the focal point for all liaisons and relationships pertaining to CIP; and 4) establish a working group, or other means of communication, to ensure that information is effectively shared between Department components having interagency relationships and liaisons.

These problems resulted in part from the CIP Task Force's cessation of operation in 2000. In addition, the IMSS did not adequately determine whether critical exchanges of information were ongoing between Department components and other entities, and it did not initiate another method of compensating for the interagency coordination program called for in the CIP Plan.

Without an effective program for interagency coordination, the Department cannot ensure effective coordination links exist and that information will be accessible from Department assets when needed.

F. Recommendations

We recommend that the Assistant Attorney General for Administration:

21. Compile a list of relationships and contacts with other federal agencies and other entities (foreign, state and local agencies, and the private sector).
22. Contact external entities to determine whether any Department assets are critical to their missions.
23. Develop and maintain a database to track liaison and interagency relationships.
24. Establish a working group to address CIP issues.

4. MEETING DEPARTMENT RESOURCE AND ORGANIZATIONAL REQUIREMENTS

The Department's CIP Plan required the identification of resources and organization requirements necessary to protect critical assets. This was to be accomplished largely through the efforts of the CIP Task Force. Although the CIP Task Force ceased operating in 2000 and never fully carried out the responsibilities in this area of the Plan, the Department has undertaken some efforts to ensure its resource and organizational requirements are adequately determined. However, full implementation of the CIP Plan has not been achieved. Studies contracted for by JMD in lieu of CIP Task Force studies have not assessed the linkage between budgetary and personnel shortfalls and the Department's critical infrastructure weaknesses. Completion of this activity is crucial to the Department's efforts to ensure that its resource and organization requirements have been met.

A. Requirement in the CIP Plan

The Department's 1999 CIP Plan provided that:

Based upon the results of the vulnerability assessments, subsequent mitigation and response plans, additional resources will have to be identified, developed, and/or procured to ensure the protection of the Department's critical infrastructure.

The purpose of this section [of the Plan] is to identify, develop, and/or procure the necessary resources to ensure the protection of the Department's critical infrastructure. Also, the section will determine and establish the appropriate organizational structure through which the protection of identified critical infrastructure assets will be implemented and sustained.

According to the Plan, the CIP Task Force or its follow-on was to begin a study to determine the appropriate organizational structure for implementing the actions called for under the Plan.

We found that the IMSS did not address the resource and organizational requirements in the April 2003 draft revision of the CIP Plan. The IMSS staff stated that there was no reason for the omission, but it is expected to be in the next CIP Plan. The CIP Plan is expected to be revised again after the Department completes its Project Matrix review.

B. Implementation of the CIP Plan for Resource and Organizational Requirements

The CIP Plan required the CIP Task Force to conduct a study in 1999 to determine the appropriate organizational structure for implementing the actions called for under the Plan. The study was to address issues such as organizational makeup (in terms of the appropriate program office representation), mission, responsibilities, intra-Department liaison, and reporting chain. The study was also to assess the linkage between budgetary and personnel shortfalls and the Department's critical infrastructure weaknesses in such areas as computer security, network security, network configuration control, aging security systems, and lack of technically qualified security professionals. However, the CIP Task Force did not accomplish the study referenced above and, as noted in Finding 1, staff of the IMSS was unable to explain why the Task Force stopped convening during calendar year 2000.

We sought to determine if the planned activities had been completed separately by JMD. JMD contracted for two studies to determine resource requirements. First, an August 7, 2000, "Operational Concept Document for Information Security Program" (Operational Concept Document) was intended to provide an assessment of the IT security program's focus and/or organization to better serve the continuously changing needs of its customer base. The resulting 17-page report discussed the critical elements necessary for a successful IT security program and presented a framework for the realignment of the Department's IT security organization. Regarding the organization for IT security, the report stated:

DOJ is comprised of many components with different focuses and interests. This very diversity accentuates the need to have an enterprise-wide Department of Justice IT security program that provides departmentwide policy, minimum-security requirements, standards, guidance, enforcement, and other value-added services to the components.

A more effective program organization would be a single organization, with a single program, where all IT is covered under a single policy, inspected against the same requirements, trained by a single training staff, subject to a single set of standards, required to undergo a consistent security process, and where all IT users have a single organization to contact for IT security assistance.

We compared the Operational Concept Document to the requirements of the CIP Plan. The Operational Concept Document met some, but not all, of the CIP Plan requirements. The Document briefly addressed organizational makeup, mission, responsibilities, and policy recommendations for computer and network security. It also presented a framework for the realignment of the Department IT security organization. However, the Operational Concept Document did not meet the plan requirements for a study of intra-Department liaisons, the reporting chain, responsibilities, and the linkage between budgetary and personnel shortfalls and critical infrastructure-specific weaknesses.

Recognizing the need for a more sophisticated study of resource needs, in light of the attacks of September 11, 2001, and the Department's crucial counterterrorism responsibilities, in July 2002 the Department contracted for an additional study, "The Information Technology Workforce Assessment" (Workforce Assessment).

In completing the Workforce Assessment, a contractor was engaged to work with the Office of the CIO to identify the additional workforce capability needs of a newly proposed CIO organization. The resulting 165-page report, dated October 15, 2002, provided assessments of human capital capabilities, human capital solutions, staffing capabilities gaps and gap-closing strategies, and an implementation plan.

We compared the Workforce Assessment to the study requirements contained in the 1999 CIP Plan as noted above. The Workforce Assessment met the plan requirements for study of organizational makeup, mission, responsibilities, intra-Department liaisons, and reporting chain. However, neither the Workforce Assessment nor the previously completed "Operational Concept Document for Information Security Program" provided an assessment of the linkage between budgetary and personnel shortfalls and the Department's critical infrastructure-specific weaknesses in such areas as computer security, network security, network configuration control, aging security systems, and lack of technically qualified security professionals. We asked the IMSS staff for an explanation as to why no assessment of linkages between budgetary and personnel shortfalls and the Department's critical infrastructure weaknesses was made but we received no response.

In summary, the October 2002 Workforce Assessment essentially completes the Department's planned 1999 activity to determine the appropriate organizational structure for implementing actions called for under the CIP Plan. Information Management and Security Staff officials indicated that they believed the CIP Plan requirement for organizational

requirements was completed in FY 2000 with the preparation of the Operational Concept Document. While we agree that the Operational Concept Document met some of the plan requirements, it was not sufficiently detailed to provide Department officials with the support needed to effectively determine resource and organizational requirements. In addition, the Department still needs to complete an assessment of the linkage between budgetary and personnel shortfalls and the Department's critical infrastructure weaknesses. Completion of this activity is crucial to the Department's efforts to ensure that its resource and organization requirements can be met.

C. Recommendation

We recommend that the Assistant Attorney General for Administration:

25. Complete an assessment of the linkage between budgetary and personnel shortfalls and the Department's critical infrastructure weaknesses.

5. ESTABLISHING EFFECTIVE RECRUITING, EDUCATING, AND AWARENESS PROGRAMS

The Department's 1999 CIP Plan recognized the need to recruit, retain, and educate both Department and contractor personnel in the areas of physical and information security. The Plan called for the completion of various programs to ensure that these needs were met. The Department has accomplished some of its efforts in the areas of recruitment, education and awareness. For example, the Department recently implemented a departmentwide initiative to provide computer security awareness training. However, we found that the recruitment and retention program called for in the Plan was not fully implemented.

A. Planned Programs

The April 1999 CIP Plan stated that the Department would establish a program to address the recruitment and retention requirements necessary for a successful critical infrastructure protection program. The Department's 1999 CIP Plan recognized the need to recruit, retain, and educate both federal and contractor personnel in the areas of physical and information security. The requirements in this area were to include creating or modifying new job series/position descriptions to ensure that individuals charged with oversight and protection of the identified critical infrastructure assets are competent and trained. This effort was also to address the retention of trained personnel in order to ensure the continuity of program execution. Training and capability requirements for individuals were to be based on national standards and criteria.

The CIP Plan also stated that the Department would establish an education, training, and awareness program specifically targeted at critical infrastructure protection. This program was to ensure that all personnel within the Department recognize their individual responsibilities for infrastructure protection and the potential outcomes of negligent actions on their part.

To accomplish the requirements of the CIP Plan, the CIP Task Force was to work with JMD Personnel Staff to develop criteria for modifying or creating a new job series in support of critical infrastructure protection. The CIP Task Force was also to work with the Department's CIO and

Security Officer to develop and promulgate training criteria and standards to ensure that individuals in key positions with the Department were proficient in their jobs, as related to critical infrastructure protection.

We found that the IMSS failed to address requirements for recruitment, education, and awareness in the April 2003 draft revision of the CIP Plan. The IMSS staff indicated that there was no reason for the omission, but they expect to include these areas in the next CIP Plan. The CIP Plan is expected be revised again after the Department completes its Project Matrix review.

B. Recruitment

We requested documentation for the recruitment and retention program established under the requirements of the CIP Plan. We were told that JMD had not established the recruitment program identified as necessary to implement a successful CIP program. We requested an explanation from IMSS staff as to why no formal recruitment program was established, but we received no response. We discussed with IMSS staff the process by which IT security personnel are recruited. We were told that the IMSS recruits for IT personnel through the Office of Personnel Management via job series GS-2210, Information Technology Specialist. Although we were told that the generic IT Specialist announcement is modified to meet the CIP role fulfilled by the IMSS, the IMSS was unable to provide copies of the modified announcements for our review.

C. Education and Training

The CIP Plan recognizes that education and training are necessary for the successful implementation of any information security program. These elements are related, but the elements involve distinctly different levels of learning. According to the CIAO's Practices for Securing Critical Information Assets guidance:

Training is geared to understanding the security aspects of the particular IT systems and applications that the individual uses. For example, all users need to learn the security features of the office automation software resident on their respective systems. Users also need to understand the security features of the local area network to which they are connected, as well as security issues related to connectivity to the Internet, intranet, and/or extranet. Education differs from training in both breadth and depth of knowledge and skills acquired. Security education, including formal courses and

certification programs, is most appropriate for an organization's designated security specialists.

The Department's July 2001 document titled, "The Information Technology Security Awareness, Training, and Education Standard and Implementation Guidelines" (Guidelines), contained minimum training requirements and implementation guidelines applying to all individuals, organizations, and entities that control, operate, maintain, and access Department of Justice systems containing SBU information.

The Guidelines generally met the requirements of the CIP Plan for training and established that full-time security professionals (regardless of job title, series, or current level of expertise) must receive 40 hours of formal security training per year and all part-time security professionals must receive 24 hours of formal security training per year. This training may include, but is not limited to, workshops, free seminars, security conferences, computer-based training, and product-specific training, as long as the total number of hours in attendance is equal to or greater than 40. However, attendance at vendor marketing briefings cannot be used to meet this requirement.

We sought to test the extent to which IMSS staff met the annual training requirement. We were told that each IT security staff member was required to have the necessary 40 hours of security training and had met that requirement annually. However, we were unable to verify this assertion because the IMSS retained documentation only for course registration and not for course completion.

D. Awareness

Security awareness can create sensitivity to the threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them. The fundamental value of IT security awareness programs is that the programs set the stage for further training by bringing about a change in attitudes, which in turn can change the organizational culture.

The IMSS has implemented an IT Security Awareness Training Initiative for the Department. As part of this effort, the Department uses a commercial off-the-shelf product, known as Computer Security Awareness Training (CSAT), to provide awareness training. The CSAT is a web-based training tool that delivers important general IT security training to all Department Government and Contractor system users. The CSAT fulfills training requirements by providing instruction on a number of security topics

such as the proper selection and protection of passwords, physical security, e-mail and Internet security, and virus protection. The Department's efforts appear sufficient to satisfy CIP requirements for computer awareness.

E. Recommendation

We recommend that the Assistant Attorney General for Administration:

26. Establish a personnel recruitment and retention program as envisioned in the CIP Plan.

6. FOLLOW-UP ON THE PRIOR OIG AUDIT OF DEPARTMENT CRITICAL INFRASTRUCTURE PLANNING FOR THE PROTECTION OF COMPUTER BASED INFRASTRUCTURE

In our November 2000 report on "Department Critical Infrastructure Protection – Planning for the Protection of Computer Based Infrastructure," we found that the Department had not yet: 1) identified all of its mission-essential assets, 2) assessed the vulnerabilities of each of its systems, 3) developed remedial action plans for identified vulnerabilities, or 4) developed a multi-year funding plan for reducing vulnerabilities. During this current audit, we tested follow-up actions taken regarding these recommendations. We found that the IMSS had completed some of the required corrective actions, but further work is required regarding the MEI inventory, plans to address weaknesses identified in vulnerability assessments, and development of a multi-year funding plan for the remediation of vulnerabilities.

PDD 63 required that the Department and other government departments and agencies prepare plans for protecting their critical infrastructure. The plans required the determination of the Department's minimum essential infrastructure, an assessment of each asset's vulnerabilities, and plans to remediate those vulnerabilities. Our prior audit focused on the adequacy of the Department's planning and assessment activities for protecting its critical computer-based infrastructure.

In our November 2000 report, we recommended that the Assistant Attorney General for Administration:

- inventory the Department's MEI in a manner that: a) uses the CIAO's definition of MEI; b) links the MEI to those Department missions that are absolutely necessary to national security, national economic security, or continuity of government operations; and c) documents the criteria used to select each asset;
- complete vulnerability assessments of the Department's MEI by December 31, 2000;
- develop remedial plans to address weaknesses identified by the vulnerability assessments; and
- develop a multi-year funding plan for the remediation of vulnerabilities.

In October 2000, JMD concurred with our findings and recommendations, and agreed to implement the appropriate corrective actions. During our current audit, we tested the extent to which the recommended corrective actions have been completed.

A. Inventory the Department's MEI

The Department revalidated its MEI in December 2002. We found that the Department utilized the CIAO's definition of MEI and a set of modified surveys to validate the MEI. Agency MEI was defined as "the framework of critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support core processes. Core processes are those that are essential to accomplishing the organization's core missions as they relate to national security, national economic security, or continuity of government services."

For each asset included in the December 2002 revalidated MEI, the IMSS provided appropriate links to the criteria and strategic goals contained in the Department's strategic plan revised as of November 2001.

The IMSS established and documented the selection criteria and procedures used in developing the December 2002 revalidated MEI. The IMSS also worked with the components in revising the MEI inventory and coordinated its activities with the CIAO. However, as noted in Finding 3 of this report, we are concerned that neither the IMSS nor the Department components considered the dependency of other government programs on the Department's IT systems, and whether critical exchanges of information were occurring. As a result, Department IT systems that exchanged critical information with external entities may not have been identified and considered adequately for protection under the CIP program.

B. Complete Vulnerability Assessments of the Department's MEI by December 31, 2000

In March 2002, the Department completed a vulnerability assessment for assets contained in the January 2001 MEI inventory. However, as discussed in Finding 1 of this report, vulnerability assessments have not been completed for assets newly added to the MEI and the assets of the ATF.

C. Remedial Plans to Address Weaknesses Identified by the Vulnerability Assessments

Finding 1 of this report details our significant concerns regarding the management of a risk mitigation program, and we provide eight recommendations regarding improvement of this program.

D. Multi-Year Funding Plan for the Remediation of Vulnerabilities

As noted in Finding 1 of this report, as part of the March 2002 Vulnerability Assessment, the Department prepared a multi-year funding plan. The Plan identifies that the Department is expected to have spent \$128 million in FY 2003 to improve IT security. However, the plan is not linked to the identified vulnerabilities and is not useful in identifying whether the funding amounts presented are adequate to remediate IT systemic vulnerabilities.

APPENDIX 1

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The primary objectives of this audit were to determine whether the Department has effectively implemented its plans for: 1) mitigating risks; 2) managing emergencies; 3) coordinating resources with other agencies; 4) meeting its resource and organizational requirements; and 5) recruiting, educating, and maintaining awareness relating to protecting its critical cyber-based infrastructures.

Scope and Methodology

The audit was performed in accordance with Government Auditing Standards, and included tests and procedures necessary to accomplish the audit objectives. We conducted work at the offices of JMD's Information Management and Security Staff located in Washington, D.C.

Our audit began July 22, 2002. To perform our audit, we conducted interviews with officials from JMD. Justice Management Division officials were from the IMSS, CSS, SEPS, and Budget Staff. Additionally, we reviewed documents related to CIP management policies and procedures, project management guidance, strategic plans, IT systems certification and accreditation, budget documentation, organizational structures, Congressional testimony, and prior GAO and OIG reports.

To determine whether the IMSS was effectively managing the CIP program, we followed guidance issued by the PCIE and ECIE Audit Committee. See Appendix 7 for description of PCIE/ECIE.

We compared the evidence collected from documents reviewed and interviews to the practices defined in the Department's CIP Plan; PDD 63; and The Practices for Securing Critical Information Technology Assets, issued by the CIAO's office. Additionally, we followed up on recommendations from our prior audit report, entitled "Department Critical Infrastructure – Planning for the Protection of Computer Based Infrastructure Report," issued November 2000. In assessing the status of the Department's effort to close the recommendations, we assessed the adequacy of: 1) the development of the MEI, particularly after the 9/11 terrorist attacks, 2) the vulnerability assessment, and 3) the multi-year funding plan.

To determine whether the Department had adequately implemented its Risk Mitigation Plan for vulnerabilities identified in the vulnerability assessment, we reviewed the vulnerability assessment, tabulated the vulnerabilities identified, tracked the status of the IMSS's efforts in monitoring mitigation activities, and noted variances. Additionally, based on comments by IMSS officials, we assessed whether resources were adequate to fund the risk mitigating activities and whether risk mitigation activities would be completed by May 2003.

In assessing the Department's implementation of their emergency management program, IMSS staff provided a description of the emergency management program. We examined the Department's management policy for: 1) indications and warnings; 2) incident collection, reporting, and analysis; 3) response and 4) contingency plans. Additionally, we attempted to verify whether these functions were adequately tested.

Our assessment of interagency coordination included a review of the methodology that the IMSS used to determine the critical support other entities' assets provide to the Department and that the Department provides to other agencies. We assessed the Infrastructure Asset Evaluation Surveys completed by Department components. Additionally, we determined the status of the development of a list of liaisons and interagency relationships as it relates to CIP.

We evaluated the Department's comparison of its organizational requirements to existing resources and the status of corrective actions or plans to correct the variances identified. We reviewed independent studies completed to analyze current organizational makeup, identify needed skills in the IT security staff, identify gaps, and propose organizational and staffing changes.

We evaluated the IMSS's current recruitment efforts and the generic criteria used to recruit IT security professionals. We reviewed resource needs identified through other reviews and, as it pertained to CIP, evaluated whether variances had been corrected.

We evaluated education and training for computer security professionals. We reviewed the generic requirements for the GS-2210, Computer Specialist, job series and evaluated the specific IMSS training requirements. We further assessed awareness policy, the purpose of which is to sensitize workers regarding the importance of security.

APPENDIX 2

ABBREVIATIONS AND ACRONYMS

ACS	Automated Case Support
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
C&A	Certification and Accreditation
CCIPS	Computer Crime and Intellectual Property Section
CIAO	Critical Infrastructure Assurance Office
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPTF	Critical Infrastructure Protection Task Force
CIS	Central Index System
CJIS	Criminal Justice Information Services
CSAT	Computer Security Awareness Training
CSIRC	Computer Security Incident Response Capability
CSS	Computer Services Staff
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
DOJCERT	Department of Justice Computer Emergency Response Team
ECIE	Executive Council on Integrity and Efficiency
EIS	El Paso Intelligence Center Information System
ENFORCE	Enforcement Case Tracking System
EPIC	El Paso Intelligence Center
FBI	Federal Bureau of Investigation
FedCIRC	Federal Computer Incident Response Center
FISA	Foreign Intelligence Surveillance Act
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GSA	General Services Administration
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
IDENT	Automated Biometric Identification System
IISNET	Intelligence Information System Network
IMSS	Information Management and Security Staff
INS	Immigration and Naturalization Service
INSINC	INS Integrated National Communications System
IT	Information Technology
ITSOWG	Information Technology Security Officers Working Group
ITSS	Information Technology Security Staff
IV&V	Independent Verification and Validation

JCN	Justice Consolidated Network
JDC-D	Justice Data Center – Dallas
JDC-W	Justice Data Center - Washington
JMD	Justice Management Division
MEI	Minimum Essential Infrastructure
MAN	Metropolitan Area Network
NADDIS	Narcotics and Dangerous Drugs Information System
NCIC	National Crime Information Center
NICS	National Instant Criminal Background Check System
NIPC	National Infrastructure Protection Center
NSI	National Security Information
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&Ms	Plans of Actions and Milestones
PCIE	President’s Council on Integrity and Efficiency
PDD	Presidential Decision Directive
SAMNET	Secured Automated Messaging Network
SBU	Sensitive but Unclassified
SEPS	Security and Emergency Planning Staff
SIOC	Strategic Information Operations Center
SMART	Security Management and Report Tool
SOD	Special Operations Division
WAN	Wide Area Network

APPENDIX 3

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

We have audited the Department's implementation of plans to protect its cyber-based infrastructure. We reviewed the Department's efforts to mitigate risks identified from vulnerability assessment; manage emergencies; coordinate with other agencies; meet its resource and organizational requirements; and assess recruitment, education, and awareness efforts.

In connection with the audit, and as required by Government Auditing Standards, we reviewed program activities and records to obtain reasonable assurance about the Department's compliance with laws and regulations that, if not complied with, we believe could have a material effect on program operations. Compliance with laws and regulations applicable to the Department's critical infrastructure planning is the responsibility of the Justice Management Division.

Our audit included examining, on a test basis, evidence about laws and regulations. Specifically, we conducted our tests against the relevant portions of:

- Presidential Decision Directive 63, The Clinton Administration's Policy on Critical Infrastructure Protection, dated May 22, 1998;
- Practices for Securing Critical Information Assets, Critical Infrastructure Assurance Office, dated January 2000;
- Department of Justice Order 2640.2D, Information Technology Security, approved July 12, 2001; and
- The Government Performance and Results Act of 1993.

Except for those issues cited in the Findings and Recommendations section of the report, our tests indicated that, for those items reviewed, the Department was in compliance with the laws and regulations referred to above. With respect to those transactions not tested, nothing came to our attention that caused us to believe that Department management was not in compliance with the laws and regulations cited above.

APPENDIX 4

STATEMENT ON MANAGEMENT CONTROLS

In planning and performing our audit of the Department's management of its planning and assessment activities for protecting its critical infrastructure, we considered the Department's management controls for the purpose of determining our auditing procedures. This evaluation was not made for the purpose of providing assurance on the management control structure as a whole; however, we noted certain matters that we consider reportable conditions under Government Auditing Standards.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the management control structure that, in our judgment, could adversely affect the Department's ability to effectively manage projects in support of its CIP planning. During our audit, we found the following management control deficiencies.

- The IMSS did not adequately oversee risk mitigation actions from components to ensure that vulnerabilities would be mitigated by May 2003.
- The Department has not ensured testing of its contingency plans for the Department's critical systems or other aspects of its emergency management plan.
- The Department has not documented its interagency and liaison relationships.
- The IMSS could not document that the Department's critical systems complied with the Department's requirements (Department Order 2640.2D).

Because we are not expressing an opinion on the Department's overall management control structure, this statement is intended for the information and use of the Department in managing its CIP program. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX 5

DEPARTMENT OF JUSTICE'S COMPUTER-BASED MINIMUM ESSENTIAL INFRASTRUCTURES

Department Component	Assets from January 2001 MEI	Assets from December 2002 MEI
DEA	El Paso Intelligence Center (EIS)	EPIC EIS
	Mercury (M2K)	M2K
	Merlin	Merlin
	Firebird	Firebird
	Model 204	Model 204
FBI		Centralized Data Intercept
		Electronic File Room
		Wide Area Network
		GESCAN
		Firebird nodes in SOD and Command Center
		Key Asset Database
		Secure Radio System
		Digital Storm Collection Systems
	Mainframe and applications	Mainframe and applications
	<i>Criminal Justice Information System (CJIS – WAN)</i>	
	<i>InfraGard</i>	
	Integrated Automated Fingerprint ID System (IAFIS)	IAFIS
	National Crime Information Center System 2000 (NCIC 2000)	NCIC 2000
	FBI Wide Area Network (FBI NET)	FBI NET
	<i>Intelligence Information System (IISNET)</i>	
	<i>Secured Automated Messaging Network (SAMNET)</i>	
INS	<i>Central Index System (CIS)</i>	
	<i>Enforcement Case Tracking System (ENFORCE)</i>	
	<i>Automated Biometric Identification System (IDENT)</i>	
	<i>INS Integrated National Communications System (INSINC)</i>	
JMD	Justice Consolidated Network (JCN)	JCN
	Justice Data Center (JDC) – Dallas Computing Platforms	JDC-D
	Justice Data Center – Washington Computing Platforms	JDC-W
		Metropolitan Area Network (MAN)

Source: Justice Management Division's 1999 CIP Plan (with added appendices) and April 2003 Draft CIP Plan

Legend: *Bold Italicized items – Deletions from MEI;*
Bolded Items – Additions to MEI

APPENDIX 6

CRITICAL ASSET DESCRIPTIONS

Component	System Name	Description
DEA	EIS	EIS is a centralized computer network comprised of a message handling system, a Geographic Information System, office automation tools, the EPIC Internal Database, and an automated external databases query capability.
DEA	Mercury	Mercury is a record message traffic system providing DEA connectivity in offices within and outside the continental United States offices.
DEA	Merlin	Merlin provides DEA intelligence analysts with access to classified information and special reports, office automation capabilities, database information, and analytical tools
DEA	Firebird	Firebird, the general support system, is the DEA office automation infrastructure upgrade initiative and provides DEA personnel with an intuitive interface for automating the investigative report process, sharing case information, and performing analysis and administrative activities.
DEA	Centralized Data Intercept	The Centralized Data Intercept serves as a central collection and distribution point for the call data information related to Title III intercepts. ⁴⁰

⁴⁰ Title III of the Omnibus Crime Control and Safe Streets Act of 1968 provided for the use of court-ordered electronic surveillance in the investigation of certain specified violations. The law provided that wiretaps could be used in emergency situations, but if a warrant was not obtained within 48 hours then any information obtained could not be used in court or even revealed.

DEA	Model 204	Model 204 Database Applications are mainframe investigative databases that support enforcement of laws.
DEA	Electronic File Room	The Electronic File Room is the central soft copy storage portion of the DEA SBU - investigative files.
DEA	Wide Area Network	DEA WAN consists of e-mail servers to support classified and SBU operations.
DEA	GESCAN	GESCAN is the DEA's automated message handling system.
DEA	Firebird nodes in Special Operations Division (SOD) and Command Center	Firebird nodes consists of Firebird NT Server, Exchange, MS Office, peripherals workstations and LAN wiring for the backup of SOD and Command Center SBU NT file services and e-mail at the offsite facility in Chantilly, VA, to NT Server.
FBI	Mainframe and Applications	The FBI mainframes contain investigative and administrative applications necessary for the FBI to perform its designated duties in securing domestic security, enforcing Federal laws, and protecting the rights and interests of United States persons.
FBI	Key Asset Database	The Key Asset Database is a database of information concerning Key Assets within each field office's jurisdiction, establish lines of communication with Key Asset owners and operators to improve cyber and physical security, and enhance ongoing coordination with other Federal, state and local government entities, to ensure their involvement in the protection of critical infrastructures.

FBI	CJIS WAN	CJIS WAN is the communications infrastructure that provides electronic connectivity between state/local law enforcement agencies, forensic/ballistic laboratories, and the FBI.
FBI	InfraGard	InfraGard is an information sharing system for computer intrusion incidents and system vulnerabilities.
FBI	IAFIS	IAFIS is a nationwide mainframe system that provides state of the art fingerprint identification processes and criminal history information for use by criminal justice and law enforcement agencies.
FBI	NCIC 2000	NCIC 2000 is the nationwide criminal justice information application that provides the law enforcement community with immediate access to documented criminal information vital to effective criminal justice operations.
FBI	Digital Storm Collection Systems	The FBI's Digital Storm Collection Systems provide for the ability to operate Foreign Intelligence Surveillance Act (FISA) Electronic Surveillance activities and collect and remotely transfer FISA information.
FBI	FBI NET	FBINET is a general support system which provides worldwide communications support to the FBI's investigative and intelligence applications at 500 locations in the United States and approximately 35 overseas locations.
FBI	IISNET	IISNET is a major application processing classified data. The system is considered to be the FBI's path for the Department of Defense TS/SCI network.

FBI	Secure Mobile Radio System	The FBI's Land Mobile Radio Systems supports secure, mobile, tactical communications throughout the United States.
FBI	SAMNET	SAMNET is a major application and processes classified data. SAMNET is a messaging system and provides access to the Defense Special Security Communications System from approximately 60 field locations.
INS	CIS	CIS is a major application. CIS contains information on persons of interest to the INS, along with summary data from other INS systems.
INS	ENFORCE	ENFORCE is an event-based case management system, integrating subject processing, biometric identification, allegations and charges, preparation and the printing of appropriate forms.
INS	IDENT	IDENT is a two-fingerprint and photo image capture identification application that enables INS offers to quickly identify persons about whom INS has information.
INS	INSINC	INSINC is the INS data communications infrastructure for non-classified processing.
JMD	JCN-MAN	The MAN provides ATM services for 22 Department resources and facilities within the D.C. metropolitan area.

JMD	JDC-D	JDC-D provides enterprise mainframe and server platform support for mission critical applications such as INS CIS.
JMD	JDC-W	JDC-W provides enterprise mainframe and service platform support for mission critical applications such as DEA Model 204 Database Applications.
JMD	JCN	JCN is a general support system providing the Department with a state-of-the-art high capacity communications backbone that consolidates individual Department components' telecommunications networks into one network to reduce costs, increase reliability, simplify network management, provide a common security approach, support emerging requirements of new applications, and foster interoperability and cooperation between components and non-Department clients.

APPENDIX 7

PCIE/ECIE DESCRIPTION

The President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) were established by Executive Order 12805, May 11, 1992, to:

- address integrity, economy, and effectiveness issues that transcend individual government agencies, and
- increase the professionalism and effectiveness of Inspector General (IG) personnel throughout the government.

To accomplish their mission, the PCIE and ECIE members look to conduct interagency and inter-entity audit, inspection, and investigation projects to promote economy and efficiency in Federal programs and operations and address more effectively governmentwide issues of fraud, waste, and abuse. The Council members also develop policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled IG workforce.

The PCIE is primarily comprised of the Presidentially-appointed IGs and the ECIE is primarily comprised of the agency head-appointed IGs. The Deputy Director for Management of the Office of Management and Budget chairs both Councils. The Chair appoints a Vice Chair from each Council to assist in carrying out its functions. Officials from the Office of Management and Budget, Federal Bureau of Investigation, Office of Government Ethics, Office of Special Counsel, and Office of Personnel Management serve on both Councils.

APPENDIX 8

THE TWELVE CRITICAL IT ASSET VULNERABILITIES

Vulnerability#1:	Lack of auditing features, audit trails, or policies and procedures.
Threat:	All threat areas can impact this vulnerability.
Discussion:	Twelve of the critical IT assets reported vulnerabilities in the area of auditing features or audit trails. In some of the systems, the auditing function was non-existent, either because it was disabled or was not a feature of the software. In other systems, the audit trail did not track activities of system users to modify, bypass, or negate system security safeguards. In some of the systems that had adequate audit features, the logs were not reviewed, there were no policies or procedures in place addressing reviewing the audit logs, or the mechanism to review the audit logs were insufficient to detect a pattern of access that would indicate a problem.
Risk Rating:	Low – moderate
Mitigation Action:	Components ensure the current IT security policy on auditing and audit trails is implemented on their critical IT assets. The IMSS will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #2:	Improper or inadequate password protection, password aging, and construction.
Threat:	All threat areas can impact this vulnerability.
Discussion:	<p>Nine of the critical IT assets have vulnerabilities related to password aging, inadequate password protection, and password construction. Some of the systems had more than one vulnerability in this area.</p> <ul style="list-style-type: none"> • Three systems had vulnerabilities related to default passwords. • Three of the systems allowed passwords that either did not meet the requirements of minimum length or did not enforce the use of alphanumeric or special characters. • Three systems had vulnerabilities associated with unencrypted passwords. • Three of the systems did not enforce the password aging policy. • Three of the systems had vulnerabilities associated with users sharing passwords.
Risk Rating:	Moderate
Mitigation Action:	Change initial login and default passwords immediately as the login passwords can be easily guessed or are widely known. Also, implement the current IT security policy on encryption, identification and authentication, and password management. Information Management and Security Staff will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #3:	Lack of Encryption.
Threat:	All threat areas can impact this vulnerability.
Discussion:	<p>Lack of encryption was cited as a vulnerability in five SBU critical IT systems. No National Security Information (NSI) [systems] had vulnerabilities related to encryption.</p> <ul style="list-style-type: none"> • Four of the systems stored and transmitted highly sensitive data without encryption, including passwords (mainframe applications). • Three systems transmit highly sensitive data without encryption across the wide area network.
Risk Rating:	Moderate
Mitigation Action:	Encrypt SBU data across general support systems because of the impact the information has on the Department's PDD 63 mission. The IMSS will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #4:	Software patches not installed for known vulnerabilities.
Threat:	All threat areas can impact this vulnerability.
Discussion:	Five systems were lacking patches to fix known vulnerabilities. ⁴¹ Exploiting known software vulnerabilities is a primary means of gaining privileged access to a system or implementing a denial of service attack.
Risk Rating:	Moderate
Mitigation Action:	Program managers should establish a program to identify, review, and install, as appropriate, patches to operating systems and other software. The patches should also be included in the configuration management documentation for the system. The IMSS will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #5:	Lack of limited or untested contingency plans.
Threat:	All threat areas can impact this vulnerability.
Discussion:	Six IT systems had vulnerabilities associated with contingency plans. The vulnerabilities included no contingency plans, limited contingency plans that addressed only one scenario, and not testing contingency plans.
Risk Rating:	Moderate
Mitigation Action:	Develop and test contingency plans for all the critical assets. The Justice Management Division has made the testing of contingency plans a performance measure for the Department and will track the progress of the individual systems within the tracking database.

⁴¹ Information Technology Laboratory Bulletin, "Computer Attacks: What They Are and How to Defend Against Them," May 1999. [This note appears in the "source" for this table.]

Vulnerability #6:	Lack of computer security incident response capability.
Threat:	All threat areas can impact this vulnerability.
Discussion:	<p>Four critical IT systems reported vulnerabilities in its Computer Security Incident Response Capability (CSIRC).</p> <ul style="list-style-type: none"> • Two systems had a draft CSIRC plan that had not been finalized. • One system did not have procedures in place for reporting incidents as required by the agency's policy. • The Computer System Security Officer for the last system did not report incidents in the time frame specified by the agency's policy.
Risk Rating:	Low
Mitigation Action:	Component Computer System Security Officers should review and ensure their CSIRC plans are current and ensure the officers are knowledgeable of the reporting requirements. The IMSS will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #7:	Lack of access controls.
Threat:	All threat areas can impact this vulnerability.
Discussion:	Seven critical IT systems reported vulnerabilities in access controls. The vulnerabilities included the failure to delete user accounts when personnel are terminated and privileges when access is no longer required due to a change of position or task.
Risk Rating:	Low – Moderate
Mitigation Action:	Components should ensure access privileges and accounts are deleted when an individual is terminated and privileges are periodically reviewed and updated based on "least privileges" and "separation of duties." The IMSS will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #8:	Lack of configuration management.
Threat:	All threat areas can impact this vulnerability.
Discussion:	Nine critical IT systems reported vulnerabilities associated with configuration management. The vulnerabilities included inadequate configuration management policies and documentation and no process to review configuration management documents on a regular basis.
Risk Rating:	Moderate
Mitigation Action:	Components should ensure system administrators for critical IT systems have established a configuration management process for their systems. The IMSS will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #9:	Lack of intrusion detection.
Threat:	All threat areas can impact this vulnerability.
Discussion:	Six critical IT assets reported vulnerabilities in the area of intrusion detection. The affected critical IT systems either did not have an intrusion detection capability, the intrusion detection system did not provide real-time monitoring, or the system did not monitor internal packet exchange traffic.
Risk Rating:	Low – Moderate
Mitigation Action:	Components should ensure their critical IT systems have an intrusion detection capability. Also, the Department established a procedure for the components to report any intrusions on their critical IT assets. The IMSS will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #10:	Lack of or inadequate virus protection.
Threat:	All threat areas can impact this vulnerability.
Discussion:	Six critical IT systems had vulnerabilities associated with lack of or inadequate virus protection. Some of the systems did not have virus protection installed on all the personal computers and network servers; other systems did not update the virus signature files on a regular basis.
Risk Rating:	Moderate
Mitigation Action:	Components should ensure the critical IT systems have virus detection software installed on all personal computers, servers, and e-mail systems, and that the software conducts a scan on a periodic basis. Additionally, the components should frequently update the protection signature files so the critical IT systems are protected from recently released viruses. The IMSS will utilize its internal database to track the resolution of this vulnerability.

Vulnerability #11:	Exploitable network services enabled.
Threat:	All threat areas can impact this vulnerability.
Discussion:	Five critical IT systems had vulnerabilities associated with exploitable network services. The network services enabled on the systems included anonymous File Transfer Protocol service, Internet Protocol forwarding, Network File System, network <i>finger</i> service, and <i>.rhosts</i> file.
Risk Rating:	Moderate – High
Mitigation Action:	Determine which services are currently running on critical IT systems, either through penetration testing or other means. Network services should be reviewed and those that are not necessary should be disabled. Appropriate countermeasures should be applied to those services that are necessary, such as “tcp wrappers” to restrict and log host access when using the <i>finger</i> network service. Components should ensure future penetration testing includes the identification of exploitable network services as a major focus of the testing. The IMSS will utilize its internal database to track the resolution of this vulnerability. In addition, for those systems that have not undergone an independent review, the IMSS will make those systems a priority for an independent review during the next 12 months.

Vulnerability #12:	Lack of warning banners.
Threat:	All threat areas could exploit this vulnerability.
Discussion:	Components of seven of the critical SBU IT assets did not display warning banners before the system sign-on screen.
Risk Rating:	Low
Mitigation Action:	Ensure all critical IT assets display warning banners before the system sign-on screen. The IMSS will utilize its internal database to track the resolution of this vulnerability.

Source: Justice Management Division’s March 2002 Vulnerability Assessment

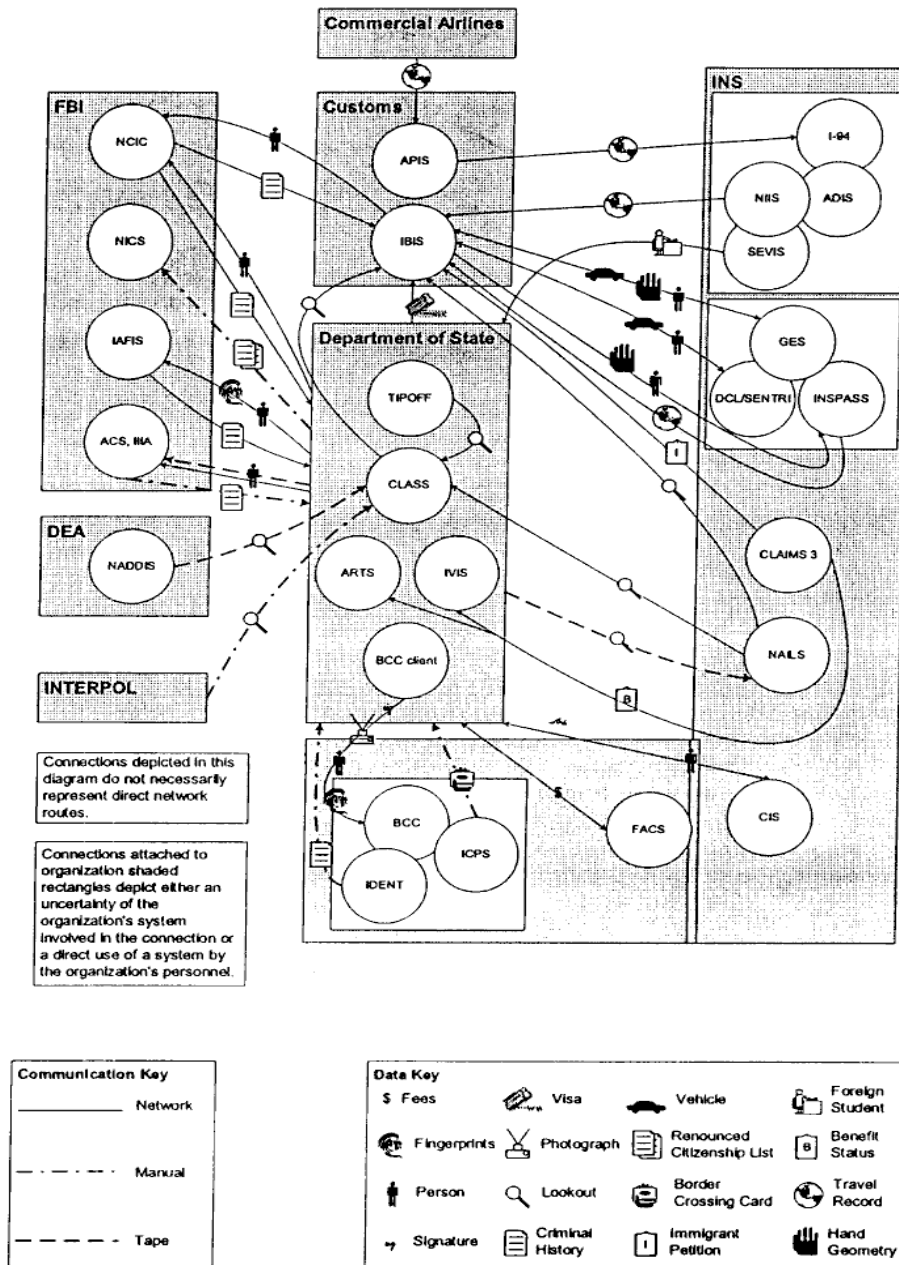
APPENDIX 9

FLOW OF INFORMATION WITH THE DEPARTMENT OF STATE AND US CUSTOMS

DRAFT - Work in Progress

November 7, 2001

Department of Justice
Information Exchanges with Department of State and US Customs



Source: Justice Management Division's November 13, 2001, Draft Information Sharing Memorandum

APPENDIX 10

DEPARTMENT ENTITIES THAT HAD CIP TASK FORCE MEMBERS

Law Enforcement:

- Criminal Division Litigation
- Criminal Division Computer Crime
- Drug Enforcement Agency
- INS
- Bureau of Prisons
- United States Marshall Service
- FBI
- Interpol
- Executive Office for United States Attorneys

Litigating Divisions:

- Civil Rights
- Antitrust
- Environmental and Natural Resource Division
- Tax Division
- Civil Division

Other:

- Office of the Deputy Attorney General
- Office of the Pardon Attorney
- Office of Information and Privacy
- Solicitor General
- Associate Attorney General
- Office of Intelligence Policy and Review
- Executive Office for United States Trustees
- Security and Emergency Planning Staff
- Office of Justice Programs
- JMD – Systems Technology Staff
- JMD – Personnel Staff
- Office of Professional Responsibility

JMD'S RESPONSE TO THE DRAFT REPORT



U.S. Department of Justice


Washington, D.C. 20530

October 10, 2003

MEMORANDUM FOR GLENN A. FINE

Inspector General

FROM:

Paul R. Corts 
Assistant Attorney General
for Administration

SUBJECT:

Response to Departmental Critical Infrastructure Protection
Implementing Plans to Protect Cyber-Based Infrastructure
Audit Report

The Justice Management Division (JMD) has reviewed the findings and recommendations in the Office of the Inspector General's (OIG) Draft Audit Report on the Department Critical Infrastructure Protection – Implementing Plans to Protect Cyber-Based Infrastructure. JMD concurs with the findings and agrees with the recommendations. Accordingly, we have made and continue to make improvements in the areas outlined in the audit.

During the 14 months of the audit, the Department's Chief Information Officer (CIO) initiated several actions that will better enable the Department to identify and protect its critical cyber-based infrastructures, and mission critical systems. These actions include revamping the Department's CIO position, including creating a Deputy CIO for Information Technology (IT) Security, reassignment of responsibility for classified system security, and initiating a Project Matrix Review with the newly formed Department of Homeland Security.

The Department originally developed its Critical Infrastructure Protection - Implementing Plan in 1999 and identified its "minimum essential infrastructure" (MEI), cyber-based assets in January 2001. Since that time the Department's missions have evolved with a stronger focus towards counter-terrorism and law enforcement information sharing. In addition, the Department's infrastructures have changed with the Immigration Naturalization Service (INS) migrating to the new Department of Homeland Security (DHS) and the Bureau of Alcohol, Tobacco, Firearms, and Explosives entering the Department.

To further develop and enhance the Department's abilities to implement the requirements of Presidential Decision Directive (PDD) 63, the Department initiated a Project Matrix Review in March 2003 with the newly formed DHS. DHS has responsibility for implementing the National Strategy on Cyber Security, and the Critical Infrastructure Assurance Office with overall responsibility for PDD 63 is maintained within DHS. Phase I of the Project Matrix Review process, expected to be completed in October 2003, will identify those functions, services, and products, whose continuing availability is vital to the United States. Phase II of the process will complete an infrastructure analysis of the critical functions and identify all assets (including cyber-based) and links (interfaces between systems and agencies). The Project Matrix process will result in a modification to the minimum essential inventory/critical asset list. Due to the impact the loss of a critical information technology (IT) asset will have on the nation, the Information Technology and Security Staff (ITSS) will start reviewing contingency plans and other documentation of IT systems as they are tentatively identified during Step 2. In addition, the ITSS will update the Department's Critical Infrastructure Protection Plan to reflect the updated mission and organization of the Department.

The JMD currently has several initiatives underway to improve its information technology security program that will, or have, implemented some of the recommendations contained in the report. Recognizing the need for an automated process to track vulnerabilities and mitigation actions, the ITSS is reviewing the capabilities of the "Automated Security Self-Evaluation and Remediation Tracking" (ASSERT) tool. ASSERT is a web-enabled process based on the National Institute of Standards (NIST) Security Self-Assessment Guide for Information Technology Systems. When implemented by JMD, ASSERT will be used to track mitigation activities for IT systems, monitor progress by component on the resolution of vulnerabilities, and monitor the status of certification and accreditation status of IT systems. ASSERT is projected to be implemented by JMD by March 2004 and populated with the major systems by May 2004.

The Department is updating the IT security policy and developing standards to implement technical, operational, and management controls in IT systems. The updated IT security policy includes roles and responsibilities for IT security personnel and requirements from the Federal Information Security Management Act (FISMA). The updated policy will replace DOJ Order 2640.2D, "Information Technology Security". ITSS is also developing seventeen technical standards based on the seventeen security controls listed in the NIST Security Self-Assessment Guide for Information Technology Systems. This includes technical standards on contingency planning and incident response. The technical standards are currently being reviewed and projected to be finalized by January 2004.

Appendix A to this document lists the five findings and twenty-six recommendations from the draft audit report. Along with the twenty-six recommendations are JMD's response and the dates corrective actions will be implemented.

Appendix A

Finding #1 Establishing a Risk Mitigation Program

1. Develop a tracking system for risk mitigation activities for classified MEI systems.

Response: JMD plans to use the Automated Security Self-Evaluation and Remedial Tracking (ASSERT) tool to track activities required to accredit an IT system. ASSERT provides for the tracking of individual vulnerabilities and mitigating actions. ASSERT will be installed on the standalone personal computer currently used to host the Security Management and Reporting Tool (SMART) classified database. The projected implementation date for ASSERT is March 2004.

2. Develop a multi-year funding plan based on resources required to mitigate vulnerabilities as identified in revised POA&Ms.

Response: JMD will not be able to identify all the Department's critical assets until the completion of Step 2 of Project Matrix, which is projected for March 2004. ASSERT is projected for implementation to track vulnerabilities, mitigation actions, and resources for classified and unclassified systems also by March 2004. However, it may take up to 60 days to populate ASSERT with the vulnerabilities, mitigating actions, and required resources for critical assets. Additionally, the mitigation plans for the critical IT systems are projected to be completed by June 2004. Therefore, the projected date to complete a multi-year funding plan for critical assets is August 2004.

3. Revise the current process used to monitor components' progress in mitigating critical IT vulnerabilities to a clear component-by-component summary of progress in mitigating vulnerabilities.

Response: The implementation of ASSERT will enable ITSS to monitor components' progress in mitigating IT vulnerabilities on a component-by-component basis. ASSERT is projected to be implemented by March 2004.

4. Monitor and document, at least quarterly, the status of certification and accreditation for critical IT systems.

Response: The ITSS is requesting funds for FY 04 to establish a "help desk" dedicated to assisting and tracking the development of certification and accreditation document by components for IT systems. The "help desk" is projected to be implemented by December 2003, and will monitor and document the status of certification and accreditation for critical IT systems.

5. *Ensure components submit proper completed POA&M in accordance with OMB guidance.*

For the use described by JMD staff, at a minimum, the component's POA&Ms should:

- a) clearly address the vulnerabilities identified in the Department Vulnerability assessment;*
- b) include the source of the vulnerabilities so readers can refer back to the Department Vulnerability Assessment to obtain additional information;*
- c) describe the performance measures used to track progress in mitigating weaknesses, and*
- d) identify resources required for implementing risk mitigation activities for each identified vulnerability.*

Response: The implementation of the ASSERT tool will ensure the components submit POA&Ms in accordance with OMB guidance. The ASSERT tool will be modified, if required, to include fields for identified vulnerabilities, the source of the vulnerabilities, performance measures to track progress in mitigating vulnerabilities, and resources required. In addition to the vulnerabilities identified in the Department Vulnerability Assessment, the system-specific POA&Ms will track all vulnerabilities, such as those identified during testing or auditing. The ASSERT tool is projected to be implemented in March 2004.

6. *Conduct vulnerability assessments and develop risk mitigation plans for assets newly added to the MEI.*

Response: The Department completed Step 1 of Project Matrix in September 2003, and has initiated Step 2. Step 2 is the identification of interdependencies of the IT systems, facilities, and personnel that are necessary for the operation of the nationally critical functions, services, and products. Step 2 is projected to be completed by March 2004. ITSS will review the vulnerability assessment of the IT systems that were added to the list to ensure they meet the requirements of PDD-63. ITSS will also assist the components in developing risk mitigation plans. The vulnerability assessments and risk mitigation plans for critical IT systems that are not adequate will be completed by June 2004.

7. *Determine the critical assets within the ATF and perform vulnerability assessments, develop risk mitigation plans, and a multi-year funding plan for those assets.*

Response: ATF was included in Step 1 of Project Matrix, and did not have any nationally critical functions, services, or products. This recommendation was completed in September 2003 when the final Step 1 report for Project Matrix was issued.

8. *Develop a work plan, with milestone dates for key activities, for attaining full operational capability for the critical infrastructure protection at the earliest possible date.*

Response: Part of attaining a full operational capability was the relocation of the DOJCERT to

ITSS, which was completed in FY 03. This allows the Department to share attack warning and information in a timely manner. ITSS will develop a work plan for attaining full operational capability by February 2004. Some of the milestones that will be included are the identification of critical assets and interdependencies based on the completion of Step 2 of Project Matrix, the review of vulnerability assessments for completeness and the development of mitigation plans, and the development of contingency plans for critical assets. ITSS has developed standards for risk mitigation, contingency planning, and incident response. The standards are currently under review and are projected to be finalized by December 2003. Additionally, ITSS project teams are developing templates for contingency plans and risk assessments to supplement the standards.

Finding #2 Establishing an Emergency Management Program

9. Define standards for secure, timely, and effective communication channels for passing indications and warning information and ensure those standards are implemented and operating.

Response: The ITSS has developed a standard for incident response which is projected to be finalized by January 2004. The standard will include the requirements for secure, timely, and effective communication channels.

10. Ensure that effective liaisons are established with the DHS's FedCIRC and the FBI's Strategic Information Operations Center and NIPC.

Response: The DOJCERT currently reports incidents and conducts liaison with the FedCIRC and the NIPC. The DOJCERT, through the Cyber Defense Operations Project Team, will contact the FBI and obtain a point of contact for incident response-related actions in the Strategic Information Operations Center by November 2003.

11. Ensure that components are in compliance with procedures for reporting incidents.

Response: The ITSS has developed a standard for incident reporting and is developing a template for incident response plans. Compliance with the standard and template will be ensured by the DOJCERT and Cyber Defense Operations Project Team reviewing the components incident response plans and reports and providing recommendations, as required. Also, the ITSS C&A "help desk" will provide assistance to the components in developing their incident response procedures and plans. The incident response reporting standard is projected to be finalized and the "help desk" implemented by December 2003. Additionally, test cases for reporting incidents are projected to be completed by February 2004 and will be used to verify reporting of incidents.

12. Ensure the data regarding department-wide computer attacks and security incidents are collected and summarized according to the nature, frequency, category, and remediation actions taken and that analyses are performed to identify potential trends and systemic weaknesses.

Response: The technical standard and template for incident response plans requires components to report incidents that meet a certain criteria to the DOJCERT and provide the report format and reporting time requirements. The technical standard and template are projected to be completed by December 2003. The DOJCERT currently conducts analysis of the incidents and provides reports on the nature, frequency, category and remediation actions taken and performs analysis to identify potential trends and systemic weaknesses. Additionally, the DOJCERT reporting and analysis processes will be evaluated on a periodic basis by ITSS using test cases developed from FedCIRC reporting requirements. The test cases are projected to be completed by February 2004.

13. Verify that incident data is provided to: a) the NIPC as part of the National Critical Infrastructure Indications and Warnings System, b) the budget processes to support and justify future CIP resource expenditures.

Response: The DOJCERT currently reports to the NIPC. The DOJCERT reporting process will be verified using the test cases described in recommendation 12. Based on incidents reports and analysis provided by DOJCERT, the ITSS will develop a list of vulnerabilities of the critical IT assets. ITSS will then review the Exhibit 300's for the critical IT systems and ensure the incident-related vulnerabilities are addressed. ITSS will initiate this process during the next submission of Exhibit 300's.

14. Verify that components have developed, implemented, and maintained internal incident response procedures and have identified appropriate individuals for reporting incidents to the DOJCERT.

Response: Currently, three components will have critical IT assets as a result of Project Matrix; the Bureau of Prisons, the Federal Bureau of Investigation, and the U.S. Marshal Service. The DOJCERT, Cyber Defense Project Team, and C&A "help desk" will provide assistance to the three components in developing their internal incident response procedures in the form of standards, templates, and document review with comments. ITSS will maintain a copy of the internal response procedures when they have been completed. Additionally, test cases verifying incident response procedures are projected to be completed by February 2004.

15. Ensure periodic testing of response plans.

Response: The Cyber Defense Operations Project Team is developing an incident response plan template, which will be completed by November 2003. Components are projected to develop and test incident response plans by June 2004. The DOJCERT and Cyber Defense Operations Project Team will assist the components in testing incident response plans.

16. Develop contingency plans for all critical IT assets.

Response: All the Department's critical IT assets will not be identified until the conclusion of

Step 2 of Project Matrix, which is projected for March 2004. However, as critical IT assets are identified during Step 2, ITSS will review the certification and accreditation documents to determine if the system has a contingency plan. If it does not, assistance in developing a contingency plan for the IT system will be a priority for the C&A help desk. Since Step 2 of Project Matrix will be completed in March 2004, contingency plans for all critical IT assets are projected to be completed by July 2004.

17. Ensure that documentation is maintained supporting the existence or development of contingency plans for all critical infrastructure assets.

Response: ITSS will review the contingency plans of critical IT assets as they are identified during Step 2 of Project Matrix. A spreadsheet will be developed and maintained by ITSS listing the status of the contingency plan (completed, under development), the date of the plan, when last tested, and comments regarding the completeness of the plan. The spreadsheet will be updated on a quarterly basis, or sooner if the contingency plans are modified. The spreadsheet will be developed by November 2003. The contingency plans will be reviewed and the spreadsheet updated as critical IT assets are identified during Step 2 of Project Matrix.

18. Verify contingency plans address all required elements as identified by Department Order 2640.2D.

Response: DOJ Order 2640.2E, which will replace DOJ Order 2640.2D, is awaiting signature. The requirements for contingency plans identified by DOJ Order 2640.2E will be included in the contingency plan standard and template. Additionally, contingency plans for critical IT systems will be reviewed by the C&A help desk. Test cases to verify that contingency plans contain the required elements are being developed and are projected to be completed by April 2004. Since all critical IT assets will not be identified until the completion of Step 2 of Project Matrix in March 2004, verification that all contingency plans contain the required elements using the test cases is projected for August 2004.

19. Obtain appropriate approvals for all contingency plans by component and IMSS officials.

Response: ITSS is currently developing a template for contingency plans. The template will include a signature page for the component approving officials and ITSS will track the validation through the ASSERT Tool. The template is projected to be completed by February 2004.

20. Test contingency plans periodically as required by Department Order 2640.2D.

Response: DOJ Order 2640.2E, which will replace DOJ Order 2640.2D, is awaiting signature. The testing of contingency plans for critical IT systems as required by DOJ Order 2640.2D or 2640.2E will be monitored by the ITSS. However, contingency plans for all critical IT systems will not be completed until November 2004, and a schedule for testing of contingency plans for all critical IT systems be developed by January 2005.

Finding # 3 Establishing an Effective Interagency Coordination Program

21. Compile a list of relationships and contacts with other federal agencies and other entities (foreign, state, and local agencies and the private sector).

Response: The components will be requested to review their service level agreements with other federal agencies and entities and provide the points of contact (with telephone numbers and email addresses), type of relationship, (supporting or supported), and summary of relationship. This information will be maintained in the database described in recommendation 23. ITSS will request the information from the components by November 15, 2003, and request they provide the information to ITSS by January 15, 2004.

22. Contact external entities to determine whether any Department assets are critical to their missions.

Response: The components will be requested to review their service level agreements (SLAs) or Memorandums of Understanding/ Memorandums of Agreement (MOU/ MOA) and contact other agencies that indicate the support provided by the Department is critical to their operation. Additionally, Step 2 of Project Matrix will identify agencies that have critical assets that are connected to Department systems. The components will be requested to review their SLAs and MOU/MOAs and provide the information to ITSS by January 15, 2004. The information on external entities will be maintained in the database described in recommendation 23.

23. Develop and maintain a database to track liaison and interagency relationships.

Response: ITSS will develop and maintain a database to track liaison and interagency relationships for critical IT systems. The database will be implemented by June 2004. The database will be populated and maintained as relationships with other agencies are established. Step 2 of Project Matrix will identify interdependencies of the Department's IT critical assets, and will probably result in the majority of the interagency relationships.

24. Establish a working group to address CIP issues.

Response: The Chief Information Officer established the Department's Information Technology Security Council (ITSC) in September 2003. The ITSC is comprised of IT security personnel from the components and is chaired by the Chief Information Security Officer, who is also the Director of ITSS. The ITSC will be used to address CIP issues. Sub-groups to address specific PDD-63 related problems will be established, as required.

Finding #4 Meeting Department Resource and Organizational Requirements

25. Complete an assessment of the linkage between budgetary and personnel shortfalls and the Department's critical infrastructure weaknesses.

Response: The completion of Project Matrix will result in a significant modification to the critical infrastructure asset list and consequently to the Department's critical infrastructure weaknesses. Project Matrix is projected to be completed by March 2004. An assessment of the linkage between budgetary and personnel shortfall and the Department's revised critical infrastructure weaknesses will be completed by December 2004.

Finding #5 Establishing Effective Recruiting, Educating, and Awareness Programs

26. Establish a personnel recruitment and retention program as envisioned in the CIP Plan.

Response : As part of its personnel recruitment and retention effort, ITSS has recently hired an individual from the Cyber Corps program, and is in the process of hiring another. The Cyber Corps is a program where graduates of a four-year academic program work for the government in return for their tuition. Both of the Cyber Corps individuals will be part of the ITSS and their duties will support parts of the critical infrastructure program, such as developing templates for risk assessments. Additionally, as part of its retention program of security professionals, ITSS sponsors the Departments seminars and testing for the Certified Information System Security Professional (CISSP) program. Five individuals from the ITSS attended the CISSP seminars and testing in FY 03. The CISSP seminars and testing hosted by ITSS trained approximately 80 IT security personnel in the Department during FY 03. The personnel and retention program as envisioned in the 1999 CIP Plan has been modified to recognize the problems of recruiting and retaining IT security professionals in a shrinking pool of qualified individuals applying for Federal positions. The current program is to provide training to current employees in the necessary skills and recruit from traditional as well as non-traditional sources such as the Cyber Corps and Presidential Appointment Interns. A formal training and retention plan is being developed by the IT Security Employee Services Project Team, which is projected for completion by September 2004.

OIG, AUDIT DIVISION ANALYSES AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

In its response to the draft report, JMD agreed with all of our audit recommendations. JMD's response to the draft audit report is included as Appendix 11 of this final report.

Recommendation number:

1. **Resolved.** This recommendation is resolved based on the JMD's plans to use the Automated Security Self-Evaluation and Remedial Tracking (ASSERT) tool to track activities to accredit IT systems. This recommendation can be closed after our review of documentation demonstrating that the ASSERT tool is being used to track risk mitigation activities for classified systems.
2. **Resolved.** This recommendation is resolved based on the JMD's plans to develop multi-year funding plans following the completion of Step 2 of Project Matrix and the implementation of the ASSERT tool to track vulnerabilities, mitigation actions and resources for classified and unclassified systems. This recommendation can be closed after our review of the multi-year funding plan linked to identified vulnerabilities for the critical assets.
3. **Resolved.** This recommendation is resolved based on the JMD's plans to use the ASSERT tool to monitor components' progress in mitigating IT vulnerabilities on a component-by-component basis. This recommendation can be closed after our review of documentation demonstrating that the ASSERT tool is being used to track IT vulnerabilities on a component-by-component basis.
4. **Resolved.** This recommendation is resolved based on the JMD's plans to establish a "help desk" dedicated to assisting and tracking the development of certification and accreditation documents by components for IT systems. This recommendation can be closed after our review of documentation demonstrating that the status of certification and accreditation for critical IT systems is being monitored at least quarterly.
5. **Resolved.** This recommendation is resolved based on the JMD's plans to use the ASSERT tool in accordance with OMB guidance and modify,

if required to include fields for identified vulnerabilities, the source of the vulnerabilities, performance measures to track progress in mitigating vulnerabilities, and resources required. This recommendation can be closed after our review of documentation demonstrating that the ASSERT tool captures POA&M data and (1) clearly addresses the vulnerabilities identified from vulnerability assessments, (2) includes the source of the vulnerabilities, (3) describes the performance measures used to track progress in mitigating weaknesses, and (4) identifies resources required for implementing risk mitigation activities for each identified vulnerability.

6. **Resolved.** This recommendation is resolved based on the JMD's plans to review the vulnerability assessment of the IT systems that were added to the list to ensure they meet the requirements of PDD-63 and the ITSS's plans to assist the components in developing risk mitigation plans. This recommendation can be closed after our review of the vulnerability assessments and risk mitigation plans for assets newly added to the MEI or documentation indicating that those assets are no longer critical.
7. **Resolved.** This recommendation is resolved based on the JMD's statement that according to the results of Step 1 of Project Matrix, the ATF did not have any nationally critical functions, services, or products. This recommendation can be closed after our review of documentation for the results of Step 1 of Project Matrix demonstrating that ATF had no critical functions, services, or products.
8. **Resolved.** This recommendation is resolved based on the JMD's plans to develop a work plan for attaining full operational capability. This recommendation can be closed after our review of the plan for attaining full operational capability.
9. **Resolved.** This recommendation is resolved based on the JMD's statement that it has developed a draft standard for incident response, which includes requirements for secure, timely, and effective communication channels. This recommendation can be closed after our review of a copy of the final standard and documentation of its implementation.
10. **Resolved.** This recommendation is resolved based on the JMD's statements that it currently reports incidents and conducts liaison with the FedCIRC and the NIPC. Additionally, JMD indicated that the DOJCERT will contact the FBI and obtain a point of contact for incident response-related actions in the Strategic Information Operations Center. This recommendation can be closed after our review of a list of liaisons JMD established with FedCIRC, the NIPC, and the Strategic

Information Operations Center. We also request for review a copy of the JMD's plans to ensure the effectiveness of the liaisons established.

11. **Resolved.** This recommendation is resolved based on the JMD's plans to have the DOJCERT and the Cyber Defense Operations Project Team review the components' incident response plans and reports. In addition, plans that the ITSS C&A "help desk" will provide assistance to the components in developing their incident response procedures and plans. Additionally, JMD intends to use test cases for reporting incidents to verify reporting of incidents. This recommendation can be closed after our review of documentation demonstrating the DOJCERT's and the Cyber Defense Operations Project Team's review of components incident response plans and reports.
12. **Resolved.** This recommendation is resolved based on the JMD's statement that DOJCERT currently conducts analysis of incidents and provides reports on the nature, frequency, category and remediation actions taken and performs analysis to identify potential trends and systemic weaknesses. This recommendation can be closed after our review of the final technical standard and template, the most recently completed examples of DOJCERT analysis and reports on incidents, and the most recently completed analysis of trends and weaknesses. We also would like to review the first evaluation by ITSS using test cases developed from FedCIRC reporting requirements.
13. **Resolved.** (a) This recommendation is resolved based on the JMD's statement and that JMD intends to verify DOJCERT's reporting process using test cases. This recommendation can be closed after our review of documentation demonstrating DOJCERT's reporting process resulting from test cases.

(b) This recommendation is resolved based on the JMD's plans to use incidents reports and analysis provided by DOJCERT to develop a list of vulnerabilities of the critical IT assets. ITSS will review the Exhibit 300's for the critical IT systems and ensure that incident-related vulnerabilities are addressed. This recommendation can be closed after our review of evidence demonstrating that results of incident report and analysis provided by DOJCERT are used in the budget process to support and justify future CIP resource expenditures.
14. **Resolved.** This recommendation is resolved based on the JMD's plans for the DOJCERT, Cyber Defense Project Team, and C&A "help desk" to provide assistance to the components in developing their internal incident response procedures in the form of standards, template, and document review with comments. This recommendation can be closed after our review of documentation demonstrating that ITSS has copies

of the internal response procedures and a list of appropriate individuals for reporting incidents to the DOJCERT.

15. **Resolved.** This recommendation is resolved based on the JMD's plans to develop an incident response plan template. In addition, the JMD plans for the DOJCERT and Cyber Defense Operations Project Team to assist the components in testing incident response plans. This recommendation can be closed after our review of documentation demonstrating tests of response plans.
16. **Resolved.** This recommendation is resolved based on the JMD's plans to review certification and accreditation documents to determine whether the system has a contingency plan, as critical assets are identified after the conclusion of Step 2 Project Matrix. This recommendation can be closed after our review of contingency plans for the critical systems.
17. **Resolved.** This recommendation is resolved based on the JMD's plans to review contingency plans as they are identified during Step 2 of Project Matrix, maintain a spreadsheet on the status of the contingency plans, and update the data quarterly. This recommendation can be closed after our review of documentation demonstrating quarterly monitoring of contingency planning.
18. **Resolved.** This recommendation is resolved based on the JMD's plans to replace DOJ Order 2640.2D with DOJ Order 2640.2E and include requirements of the new order in the contingency plan standard and template. Additionally, the JMD intends to have the contingency plans reviewed at the C&A "help desk" and to use test cases to verify that contingency plans contain the required elements. This recommendation can be closed after our review of documentation demonstrating that contingency plans for critical IT assets address all required elements.
19. **Resolved.** This recommendation is resolved based on the JMD's plans to develop a template for contingency plans. The template is expected to include a signature page for the component approving officials and ITSS will track the validation through the ASSERT tool. This recommendation can be closed after our review of documentation demonstrating that the contingency plans for the critical IT assets have been approved by the appropriate officials.
20. **Resolved.** This recommendation is resolved based on the JMD's plans to develop a schedule for the testing of contingency plans for all critical IT systems and to monitor those tests. This recommendation can be closed when receive documentation demonstrating that the contingency plans for the critical IT assets have been tested.

21. **Resolved.** This recommendation is resolved based on the JMD's plans to develop and maintain a database to track liaison and interagency relationships for critical IT systems. This recommendation can be closed after our review of documentation demonstrating that a database has been developed to track liaison and interagency relationships and has been populated.
22. **Resolved.** This recommendation is resolved based on the JMD's plans to request that components review their service level agreements or Memorandums of Understanding and contact other agencies that indicate the support provided by the Department is critical to their operation. Additionally, Step 2 of Project Matrix will identify agencies that have critical assets that are connected to Department's systems. This recommendation can be closed after our review of documentation demonstrating that the Department has identified which of its assets are critical to other agencies.
23. **Resolved.** This recommendation is resolved based on the JMD's plans to develop and maintain a database to track liaison and interagency relationships for critical IT systems. This recommendation can be closed after our review of documentation demonstrating that a database for tracking liaison and interagency relationships for critical IT systems have been developed and populated.
24. **Resolved.** This recommendation is resolved based on the JMD's statement that it has established the Department's Information Technology Security Council (ITSC). The ITSC will be used to address CIP issues. This recommendation can be closed after our review of documentation demonstrating that the ITSC is addressing CIP issues.
25. **Resolved.** This recommendation is resolved based on the JMD's plans to complete an assessment of the linkage between budgetary and personnel shortfall after the completion of Project Matrix and consequently to the Department's critical infrastructure weaknesses. This recommendation can be closed after our review of documentation demonstrating that JMD has completed an assessment of the linkages between budgetary and personnel shortfalls and critical infrastructure weaknesses.
26. **Resolved.** This recommendation is resolved based on the JMD's statement that it has hired an individual from the Cyber Corps Program and is in the process of hiring another. Both of the Cyber Corps individuals will be part of the ITSS and their duties will support parts of the critical infrastructure program, such as developing templates for risk assessments. Additionally, as part of its retention program of security professionals, ITSS sponsors the departments seminar and testing for the Certified Information System Security

Professional program. A formal training and retention plan is being developed by the IT Security Employee Services Project Team. This recommendation can be closed after our review of a copy of the formal training and retention plan.